OpenPGP Tutorial

Step by Step Walkthrough Using Kleopatra

Date March 8, 2023

Author:

Change Authority: EFX Data Protection/NIST

Change Forecast: As needed per NIST Standards

This document will be kept under revision control.

Change History

Version No.	Issue Date	Status	Reason for Change
PGPKLEO.2021.1	2023-0...	Submitted	Initial Release
PGPKLEO.2023.1	2023-0...	Submitted	Update - New EFX PGP Rqmnts

Reviewer History

Reviewer's Details	Version No.	Date
Geoffrey Lewis	PGPKLEO.2021.1	2021-02-25
Nick Fuller	PGPKLEO.2023.1	2023-03-09
Benjamin Hale	PGPKLEO.2023.1	2023-03-09
Geoffrey Lewis	PGPKLEO.2023.1	2023-03-09

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.

Table of Contents

Table of Contents 2
1. Introduction 3
2. Installation 4
3. Generating a New Key Pair 6
4. Locating, Verifying, and Exporting Public Key 9
5. Exporting and Backing Up Private Key 12
6. Importing a Public Key 13
7. Encrypting Files Sent to Equifax 15
8. Decrypting Files Sent from Equifax 17

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.

1. Introduction

1.1. What is Pretty Good Privacy (PGP)? is a tool for keeping your data safe.
- 1.1.1. PGP was a popular program used to encrypt and decrypt email over the internet, as well as authenticate messages with digital signatures and encrypted stored files.
- 1.1.2. PGP now commonly refers to any encryption program or application that implements the OpenPGP public key cryptography standard.
- 1.1.3. PGP allows users to encrypt (scrambles) their data so no unauthorized person is unable to read the information.

1.2. PGP makes use of four types of keys:
- 1.2.1. One-time session symmetric keys
- 1.2.2. Passphrase-based symmetric keys
- 1.2.3. Asymmetric keys (public/private key pair)

1.3. How is PGP implemented at Equifax?
- 1.3.1. Equifax uses asymmetric PGP keys for PGP encryption/decryption.
- 1.3.2. PGP encryption is performed with the public key.
- 1.3.3. PGP decryption is performed with the private key pair for that public key.
- 1.3.4. Authorized users must have access to the Only you and Equifax will have access to the decrypted (unscrambled) information.

1.4. PGP Key Requirements
- 1.4.1. PGP key length is 2048+ bits.
- 1.4.2. PGP key is created in RSA format.
- 1.4.3. Public PGP key block contains both primary and sub keys.
- 1.4.4. PGP key contains an expiration date no later than 2 years after create date.
- 1.4.5. AEAD feature is removed (Preferred, not Required)

1.5. PGP Encryption Requirements
- 1.5.1. Cipher Algorithm is AES256.

1.6. What will I learn in this PGP walkthrough?
- 1.6.1. You will learn to create and apply a PGP key pair that meets Equifax requirements.
- 1.6.2. Import and encrypt files sent to Equifax that meet its PGP encryption requirements.
- 1.6.3. Decrypt PGP encrypted files received from Equifax.

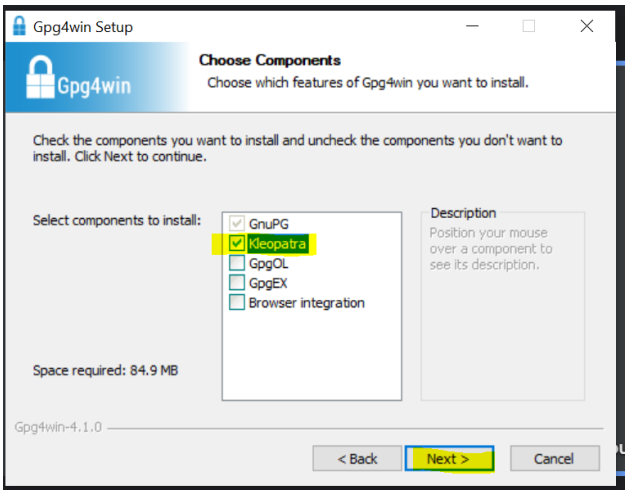
1.7. Does Equifax own, maintain, or promote Kleopatra or any other OpenPGP related product?
- 1.7.1. Equifax does use OpenPGP for all client batch file level encryption/decryption.
- 1.7.2. Equifax does not recommend any specific OpenPGP file encryption software.
- 1.7.3. Equifax does suggest, however, that clients 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.

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.

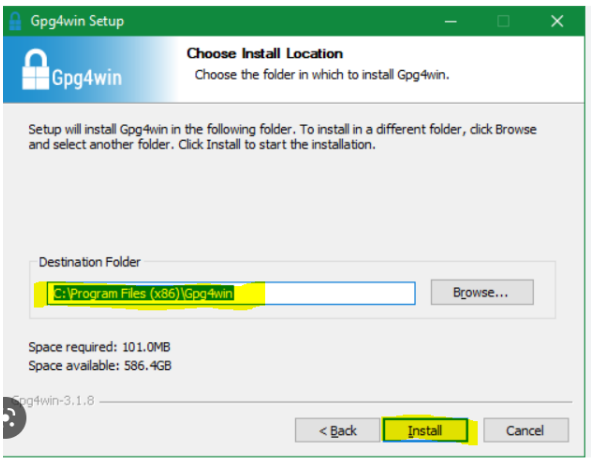
2. Installation

2.1. Download GPG4WIN from https://www.gpg4win.org/download.html , then run the install. Select your language and Click Next.

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



2.3. Click Next> then click Install.



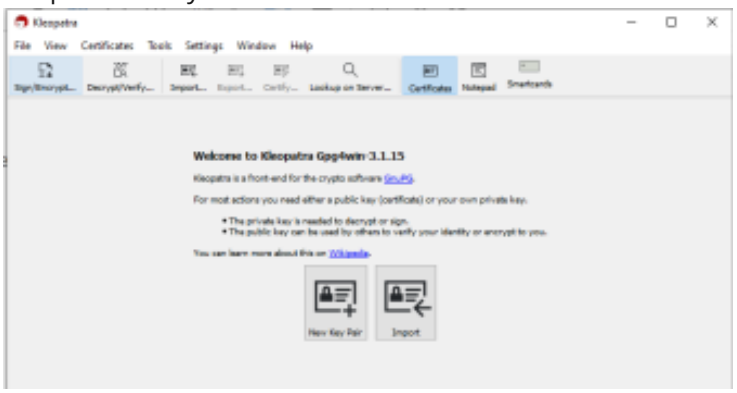
2.4. Once setup is done, check the 'Run Kleopatra' box. Click Finish.

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.

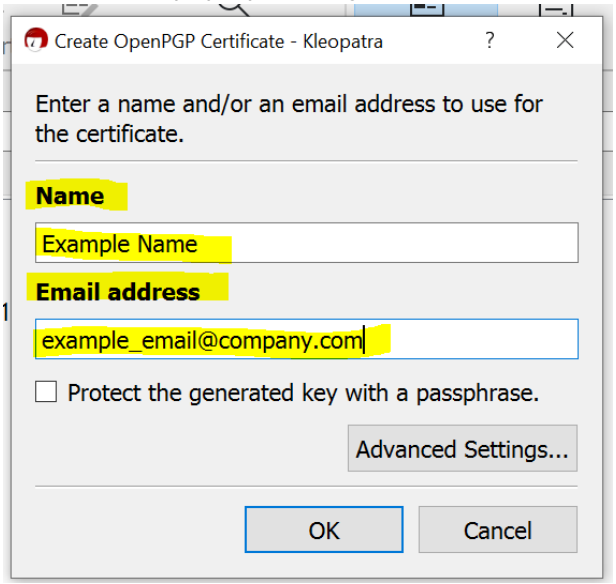
IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

3. Generating a New Key Pair

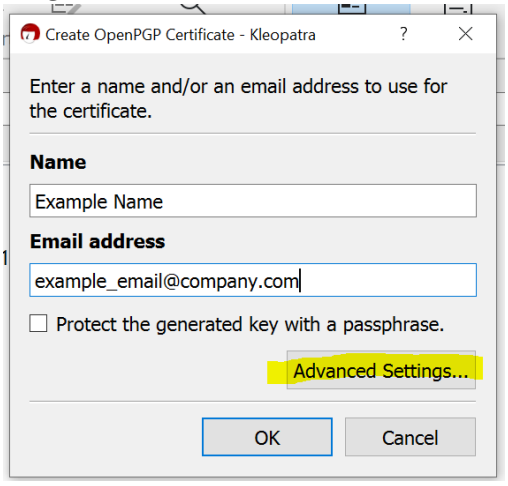
3.1. Once the setup is done, you will see this screen, click New Key Pair. If you do not see the below screen, go to File → New OpenPGP Key Pair…



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

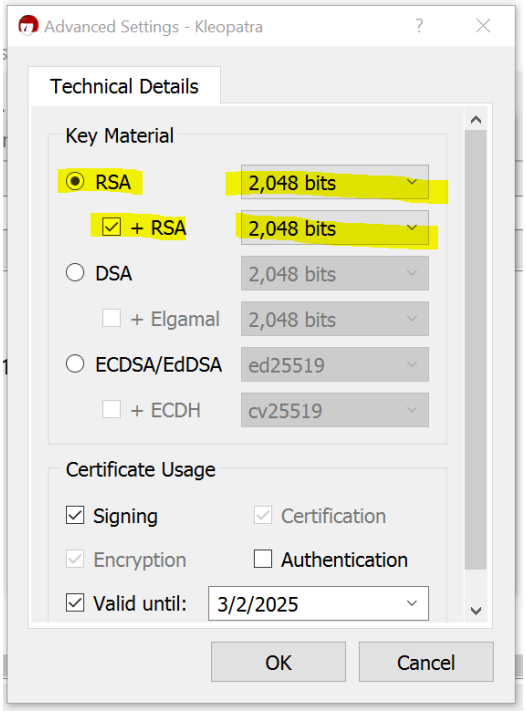


3.3. Click Advanced Settings.

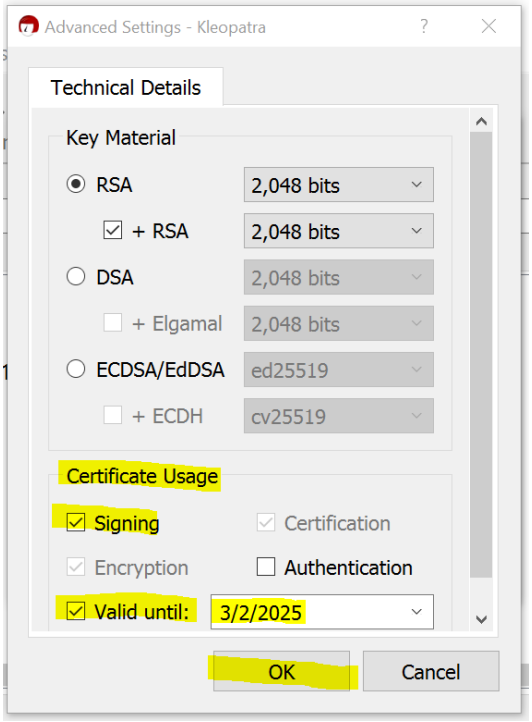


IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

3.4. Under Key Materials, select RSA, check the "= RSA" checkbox, select 2,048 bits from the two dropdowns.

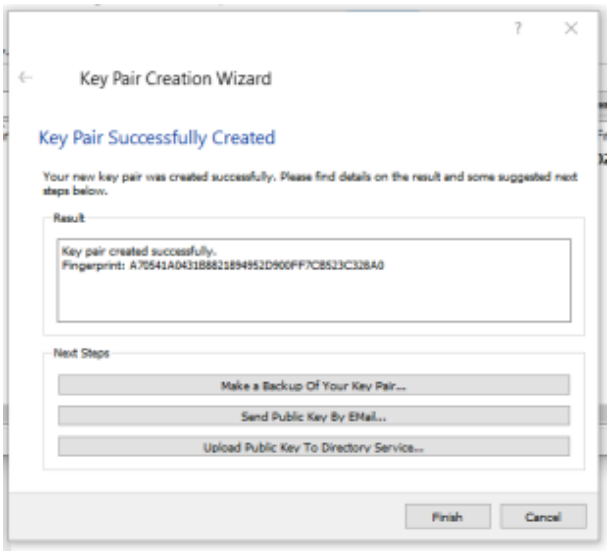


3.5. Under Certificate Usage, check the "Signing" checkbox, check the "Valid until" checkbox, select an expiration date that is no later than two years from the date the key pair is being created. Click OK.



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.

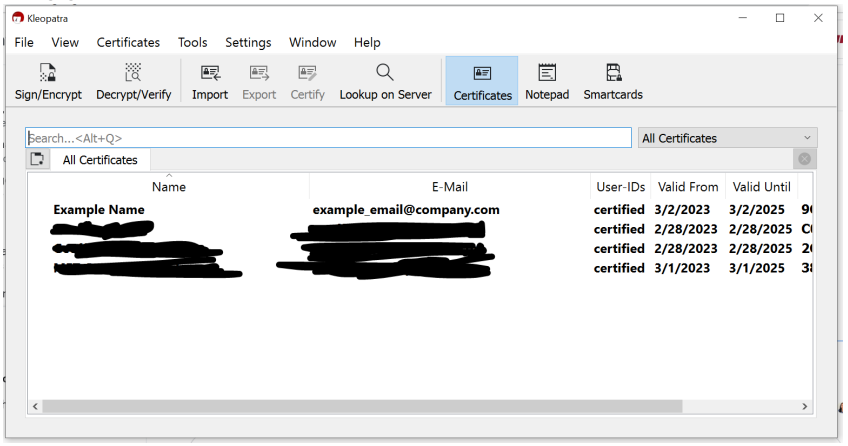
3.6. You should receive the below screen showing Key Pair Successfully Created. Click Finish.



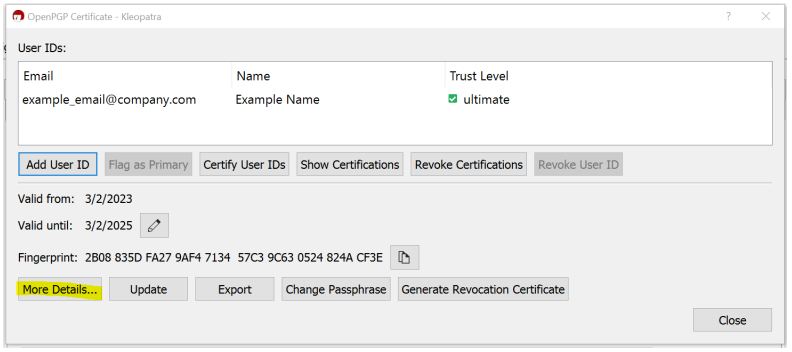
IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

4. Locating, Verifying, 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 and double click it.

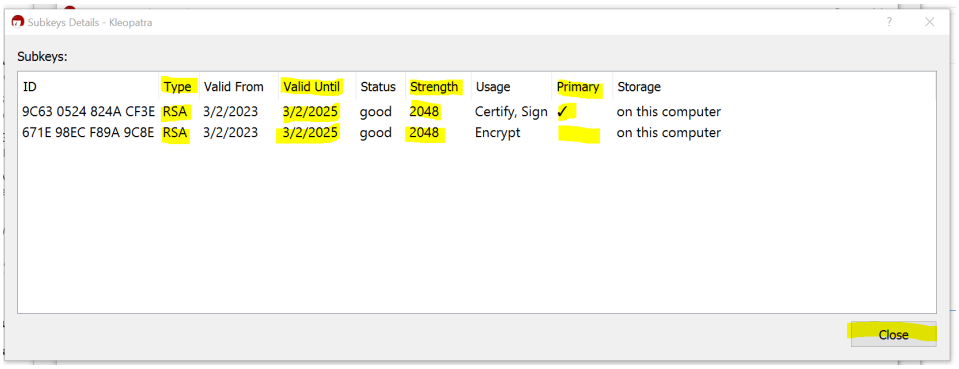


4.2. You will see the screen shown below. Click More Details....



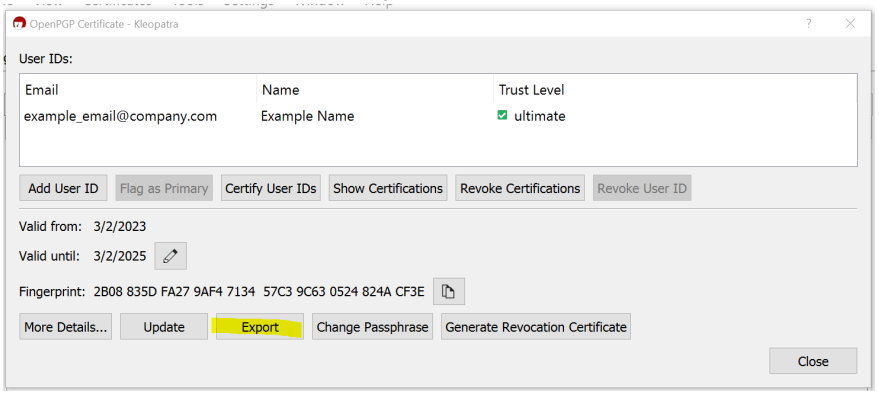
4.3. You will see the screen shown below. From here you can verify the below Equifax requirements are met. If so, click Close.

Type = RSA
Valid Until date is no later than two years after Valid From date
Strength = 2048 or higher
You see both Primary key (Primary = check) and subkey (Primary = unchecked)

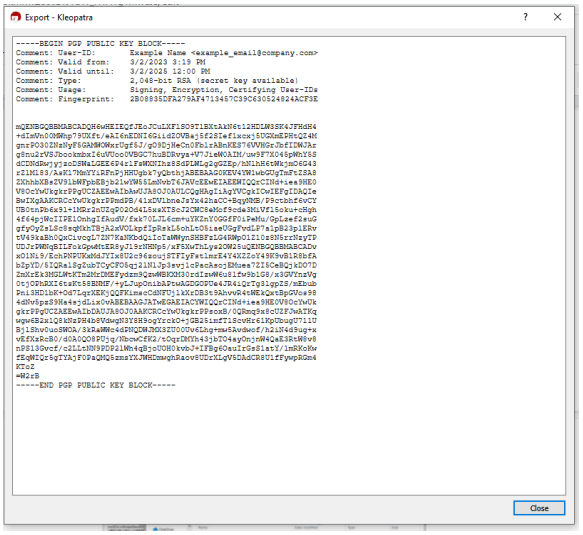


IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

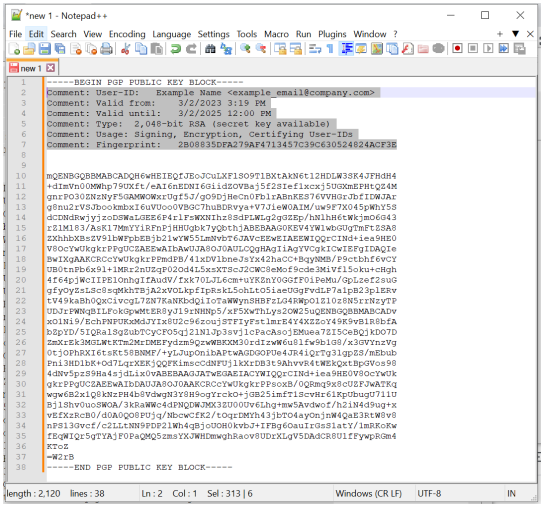
4.4. From the below window, click Export.



4.5. You should be able to see your public key. Copy the entire key block and Paste the PGP Key Block into any document editor NotePad++, Word, Wordpad, etc.) that allows you to Save As a .txt file.

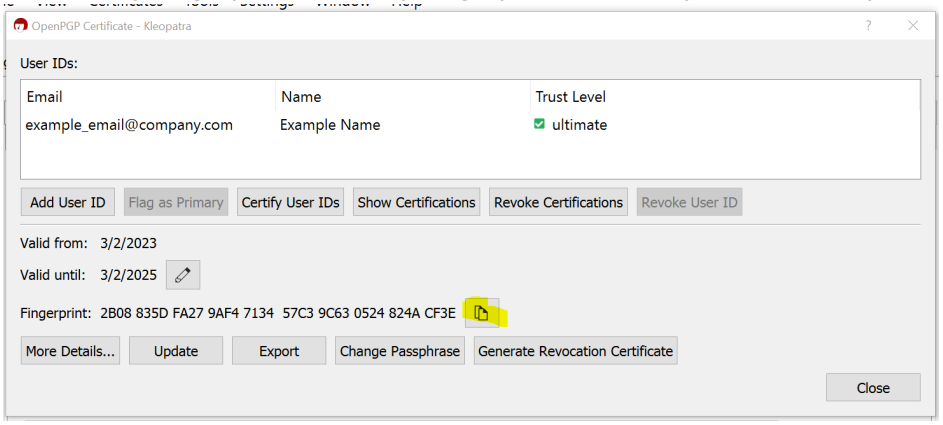


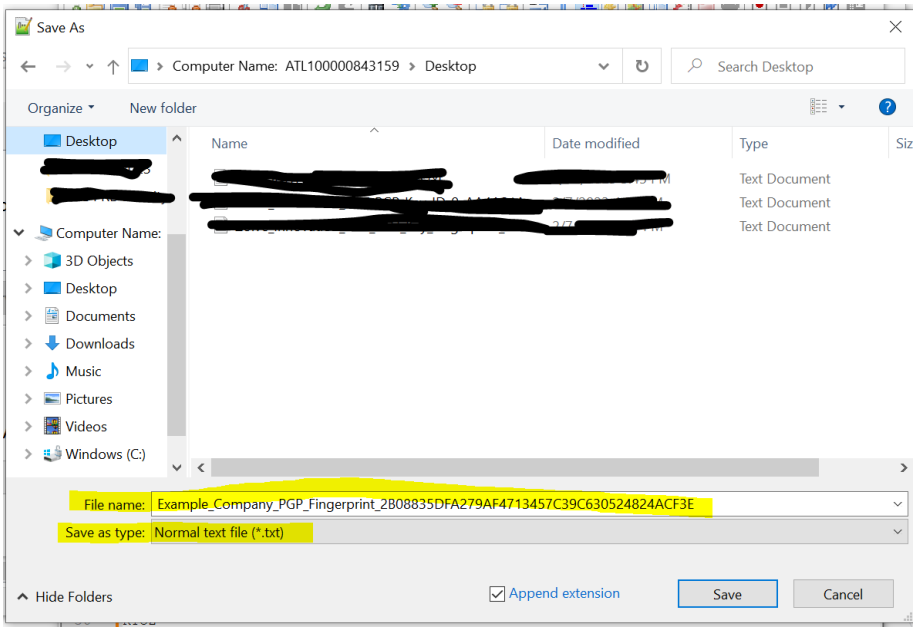
4.6. Delete all" Comment:" lines prior to saving.



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.

4.7. Save as a .txt file using a file naming convention that includes your company name PGP Key Fingerprint. PGP Key Fingerprint can be copied from Kleopatra.





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

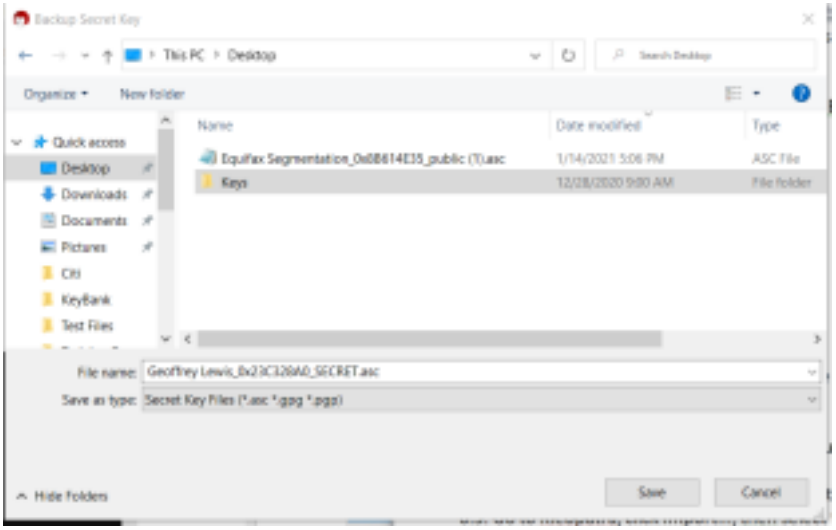
IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

5. Exporting and Backing Up Private Key

NOTE: Keep your private key secret, NEVER share a private key!!! However, it's recommended by Kleopatra developers to back up your private key, in case of computer failure, theft or accidental deletion.

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

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

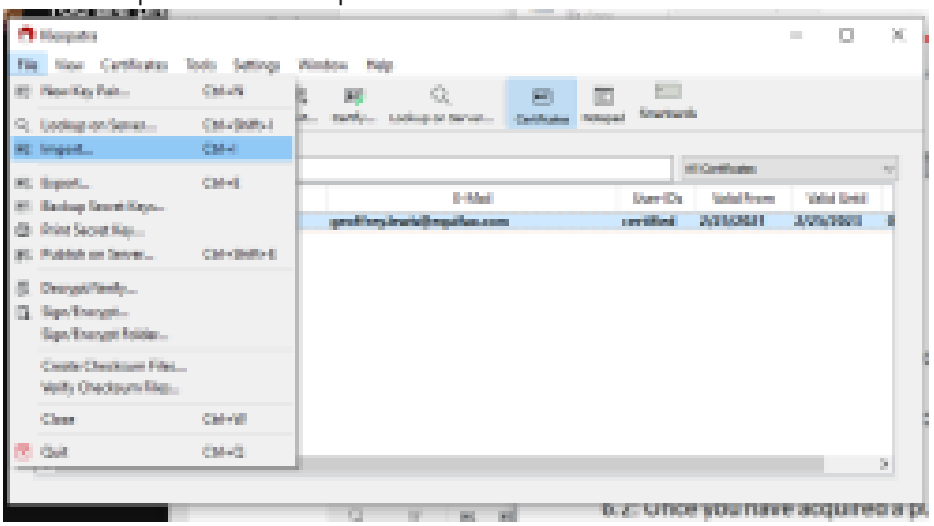


IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

6. Importing a Public Key

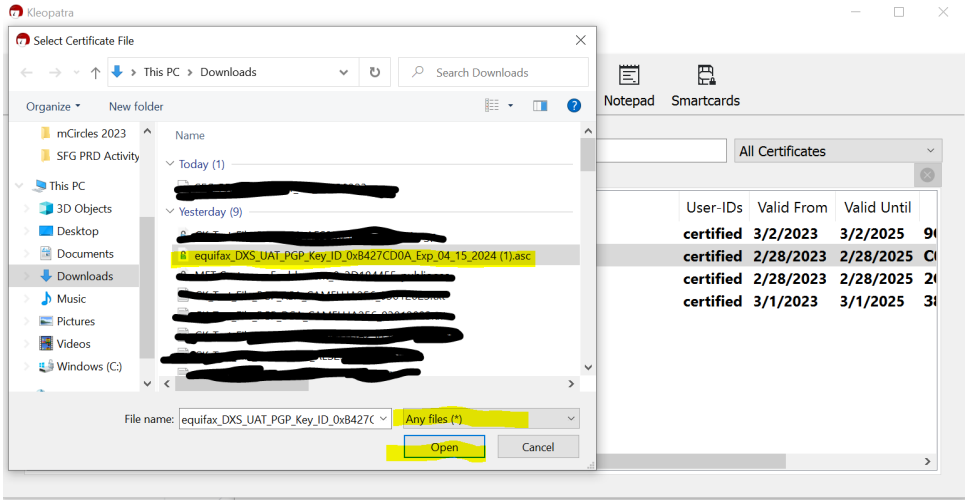
6.1. To send Equifax an encrypted file, you must import and certify both the Equifax SFG UAT PGP Key and SFG PRD PGP Key. Equifax should provide you the keys as email attachments. Download both keys from your email and save on your local drive.

6.2. Go to Kleopatra File Import...



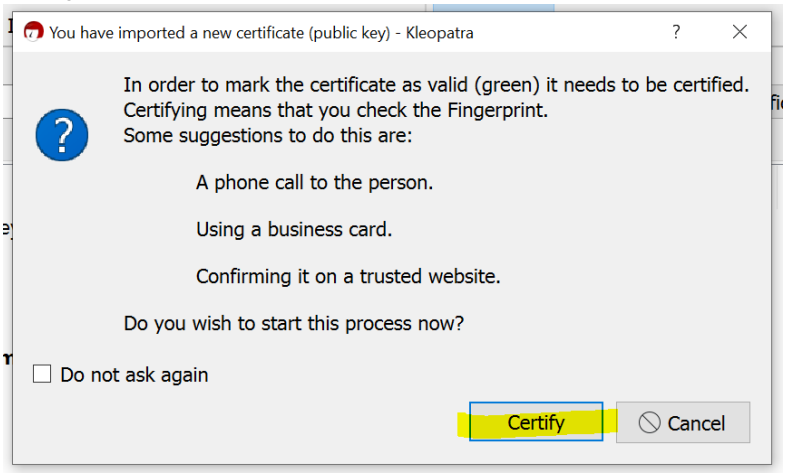
6.3. Go to the directory where you saved the keys and select them. Change the file type to any type in order to view the keys.

6.4. Click Open.

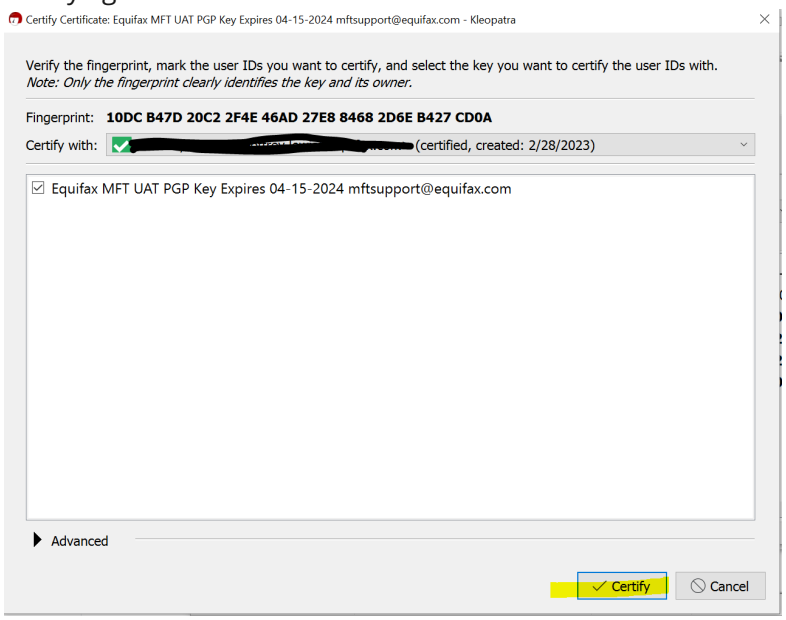


IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

6.5. Click Certify.



6.6. Click Certify again.

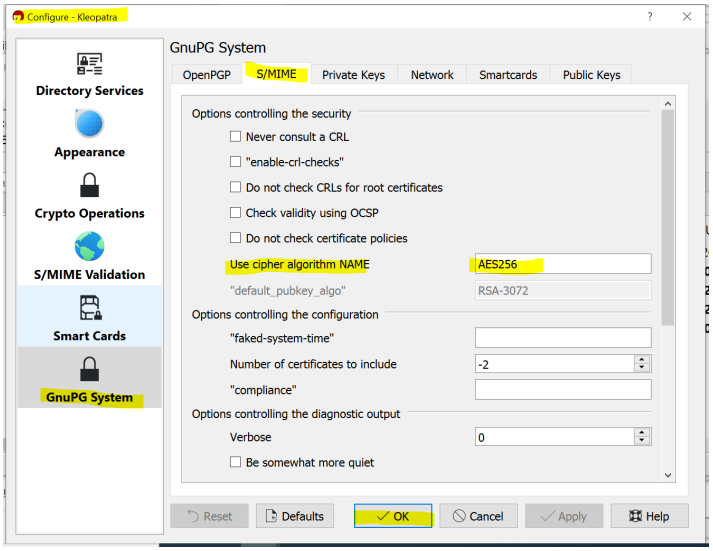


6.7. Repeat steps 6.1 - 6.5 as needed.

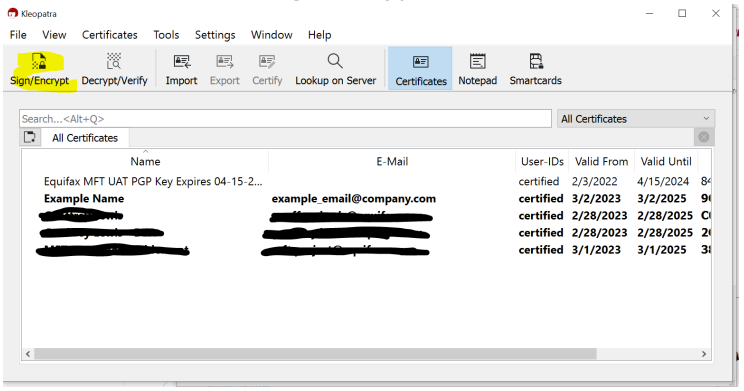
IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

7. Encrypting Files Sent to Equifax

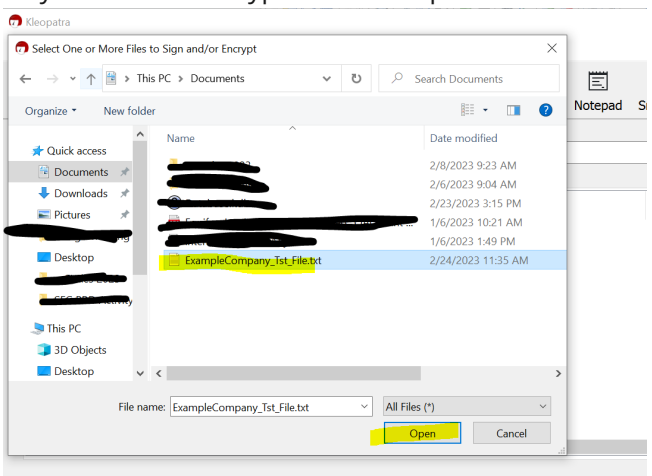
7.1. Go to Settings → Configure Kleopatra → GnuPG System → S/MIME. Ensure "Use cipher algorithm NAME" is AES256. If not, Type AES256 in the free text field and click OK.



7.2. From the home screen, click Sign/Encrypt....

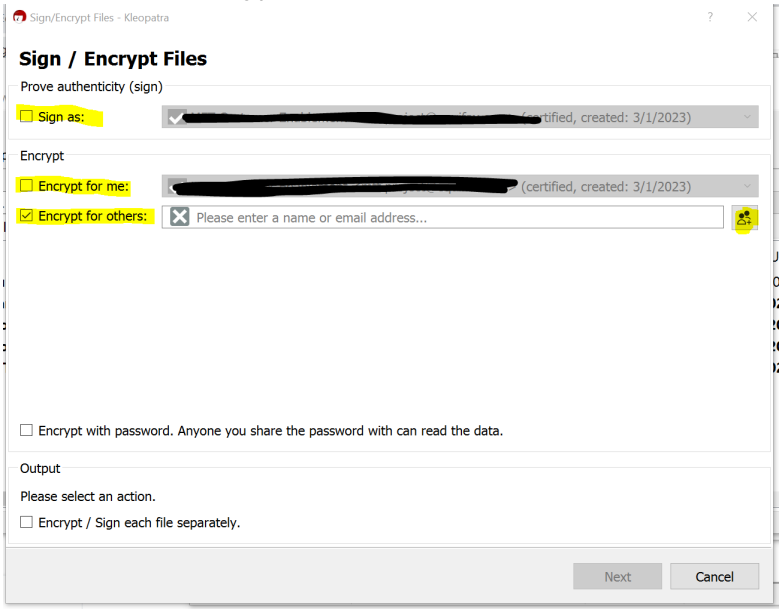


7.3. Select the file you want to encrypt and click Open.

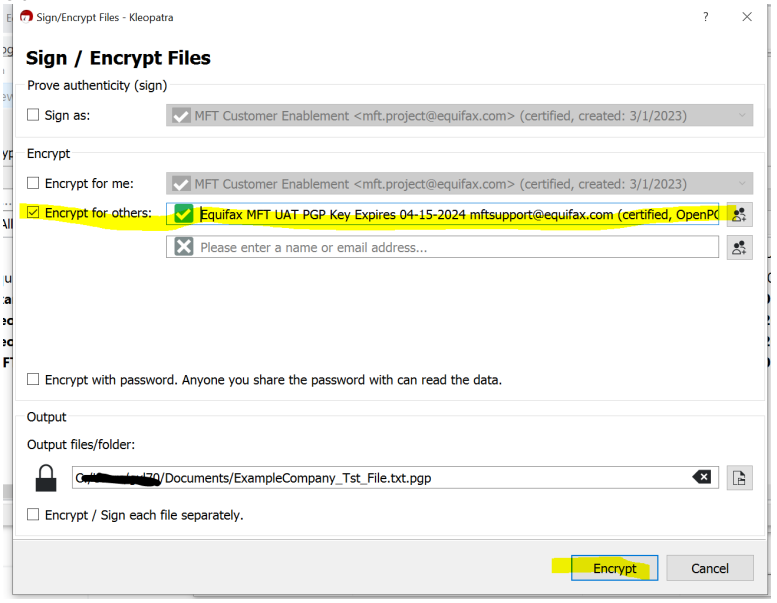


IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

7.4. From the below screen, uncheck “Sign as”, uncheck “Encrypt for me”, check “Encrypt for others”, click on the people icon to the right and select the public key you want to use for encryption.



7.5. Click Encrypt.

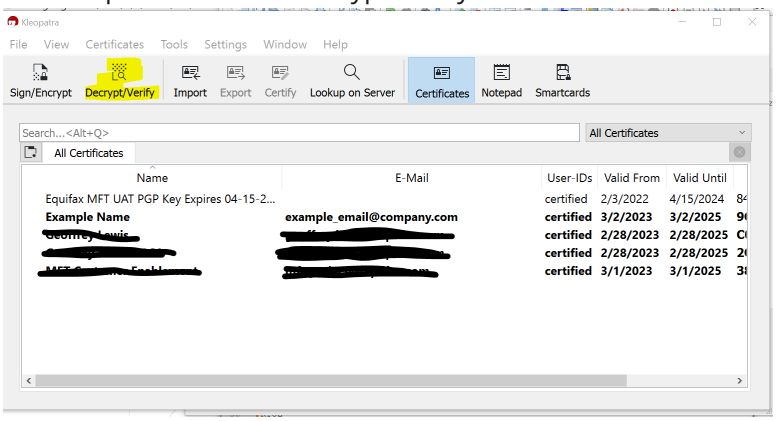


IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

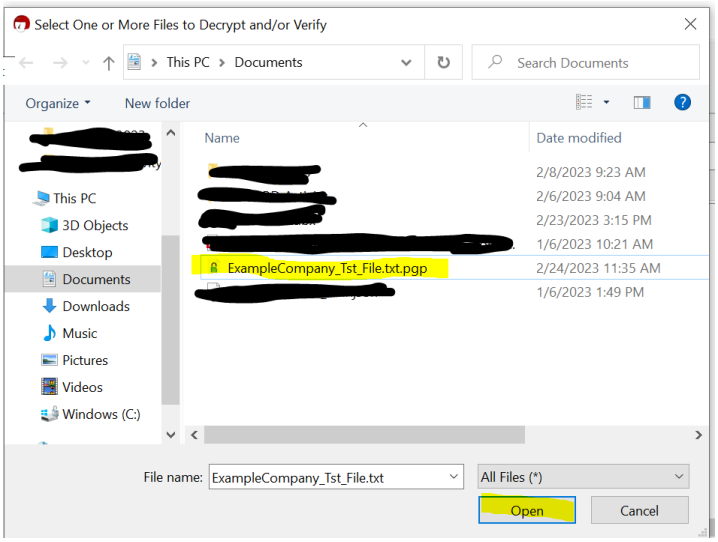
8. Decrypting Files Sent from Equifax

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

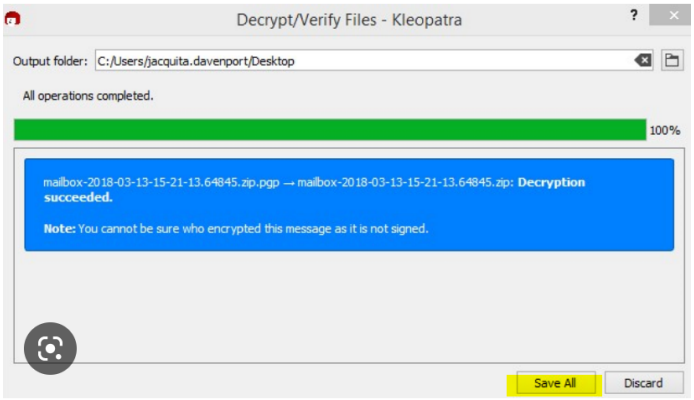
8.2. Go to Kleopatra and click Decrypt/Verify…



8.3. Select your encrypted file and click Open.



8.4. Once you see the success screen below, click Save All. 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.