



OpenPGP Tutorial

Step by Step Walkthrough Using Kleopatra

Date March 1, 2024

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.

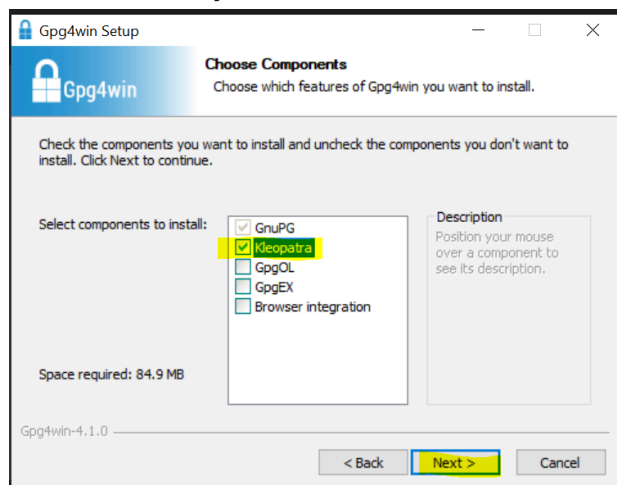
IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

2. Installation

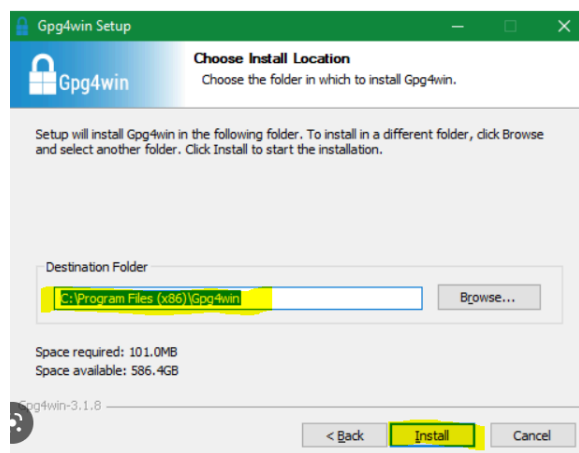
- 2.1. Download GPG4WIN from <https://www.gpg4win.org/download.html> , then run the install. Select your language and Click Next.



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

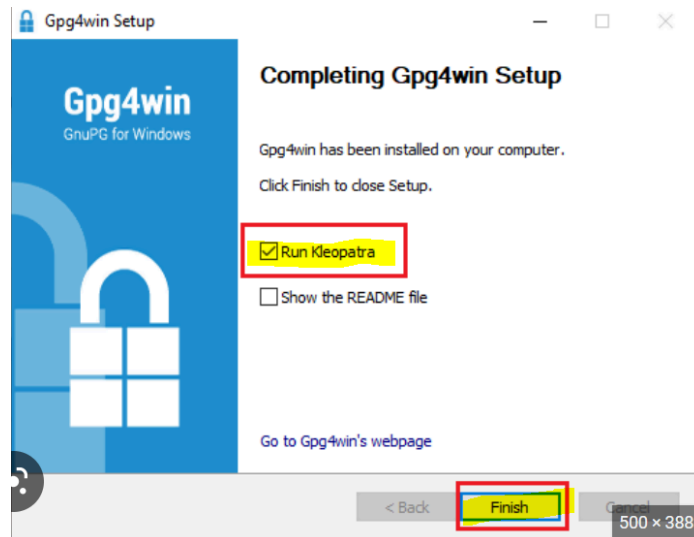


- 2.3. Click Next> then click Install.



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.

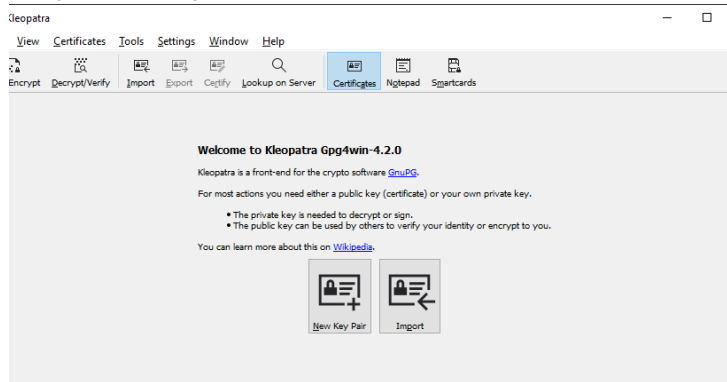
2.4. Once setup is done, check the 'Run Kleopatra' box. Click Finish.



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 a New Key Pair

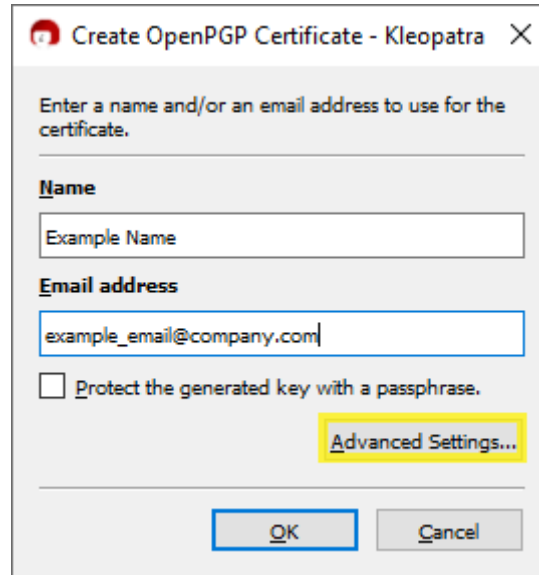
- 3.1. Once the setup is done, you will see this screen, click New Key Pair. If you do not see the below screen, go to File → New OpenPGP Key Pair...



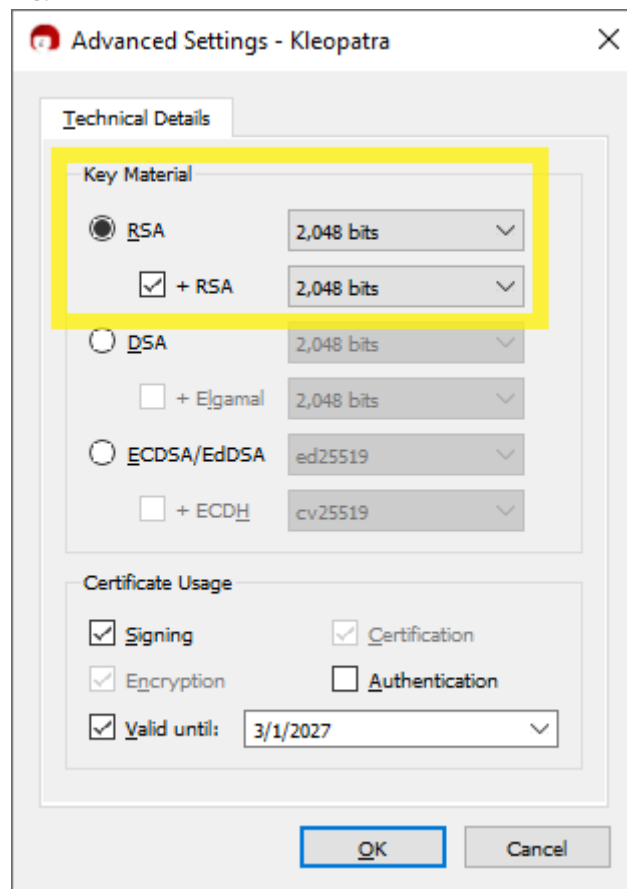
- 3.2. Screen shown below will pop-up. Enter your name and email.

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.

- 3.3. Click Advanced Settings.

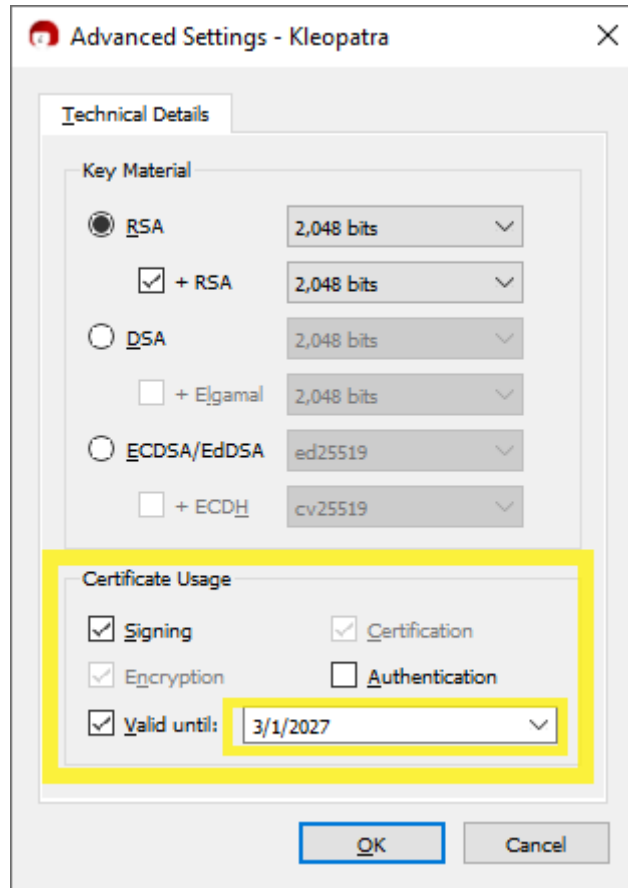


- 3.4. Under Key Materials, select RSA, check the “= RSA” checkbox, select 2,048 bits from the two dropdowns.

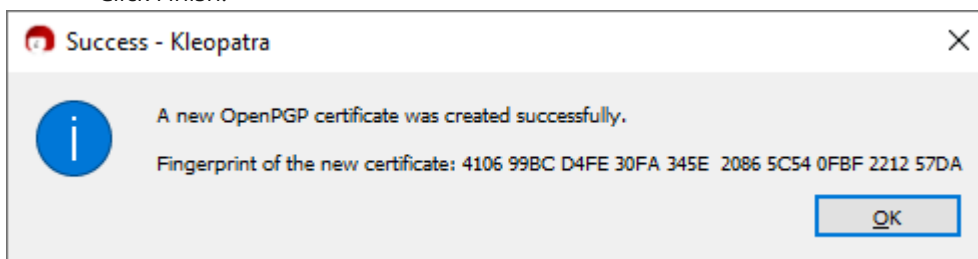


IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

- 3.5. 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.



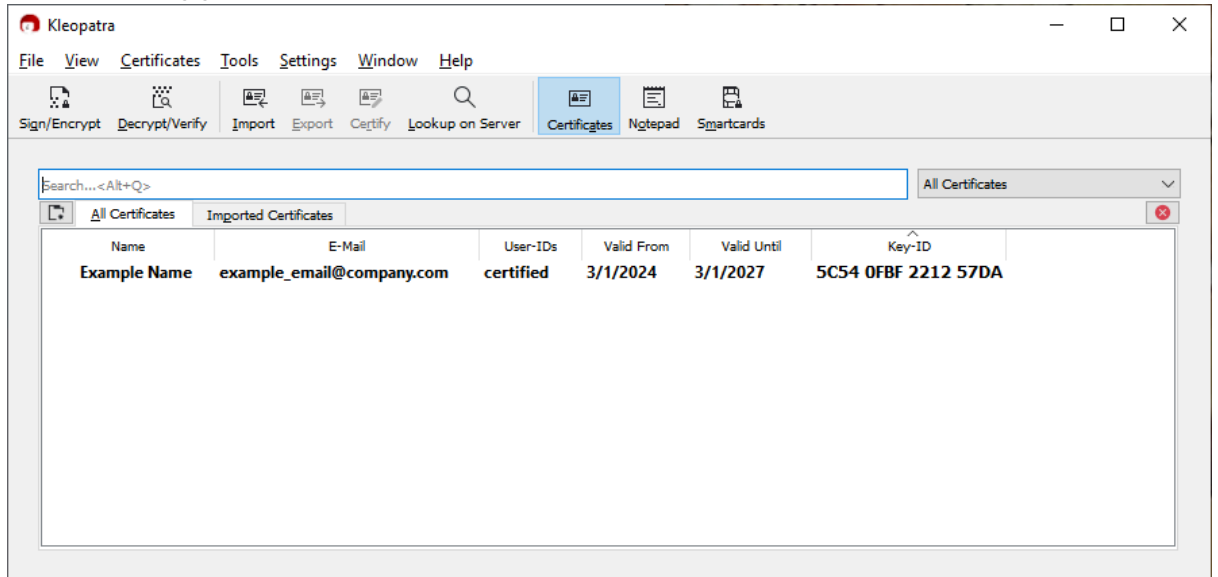
- 3.6. You should receive the below screen showing Key Pair Successfully Created. Click Finish.



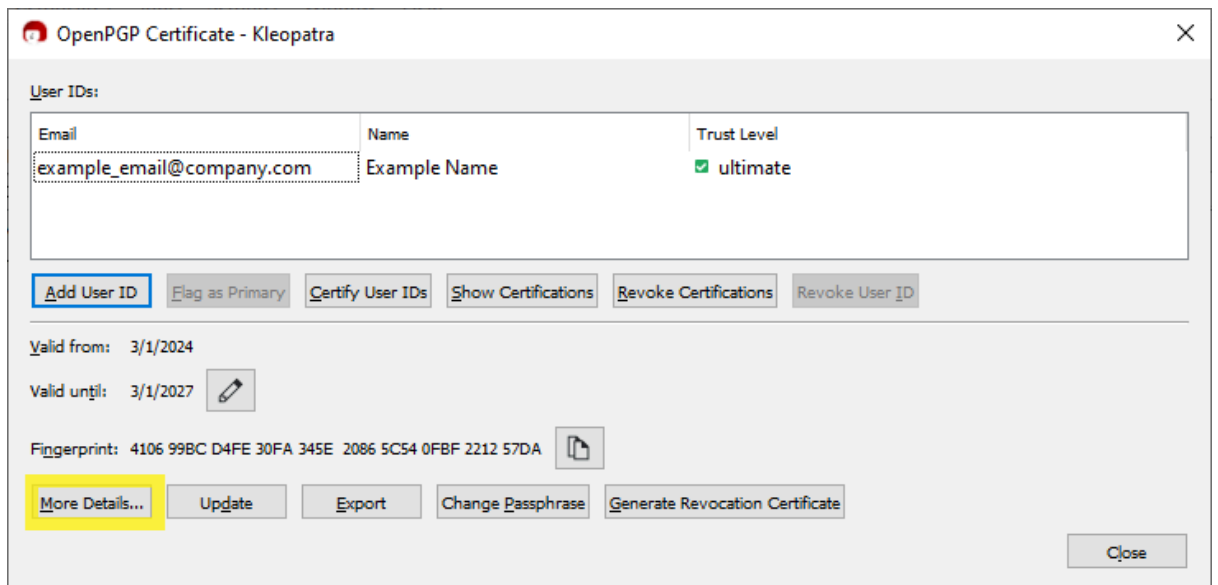
IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

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....



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.

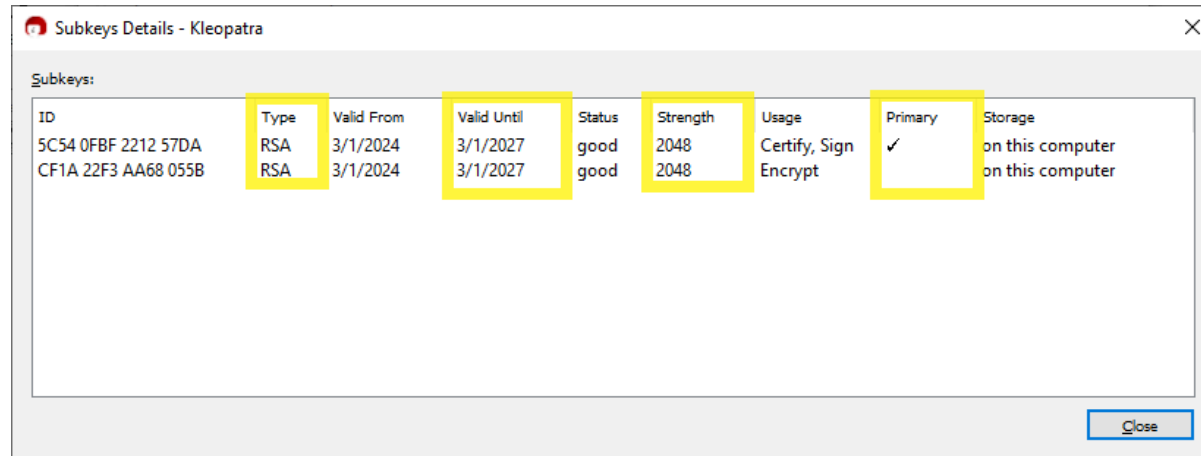
4.3. You will see the screen shown below. From here you can verify the below Equifax requirements are met. If so, click Close.

Type = RSA

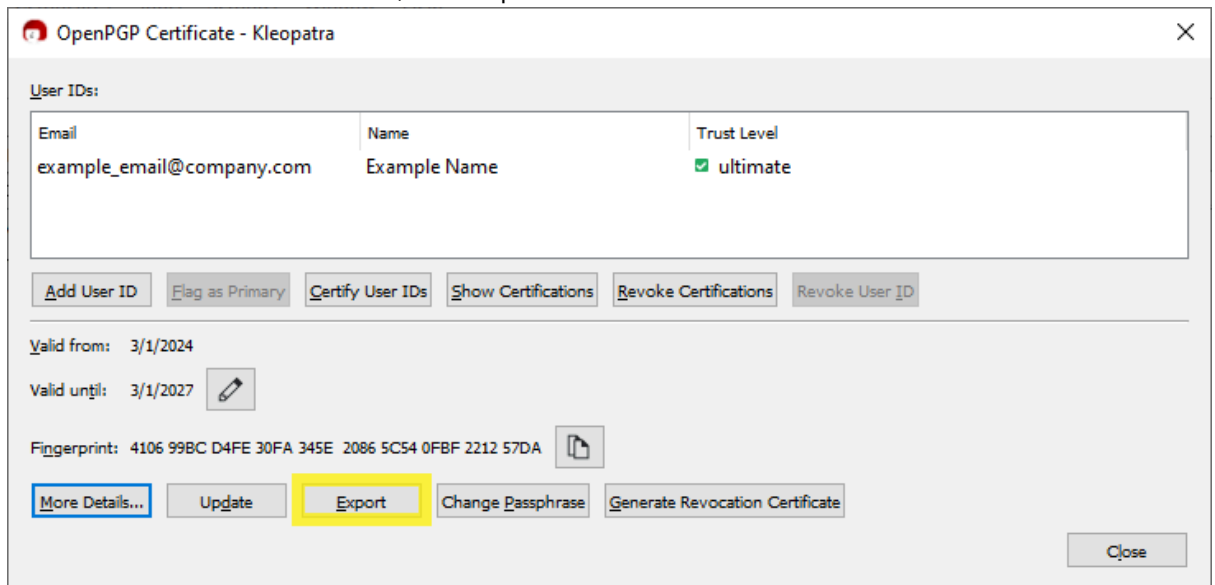
Valid Until date is no later than two years after Valid From date

Strength = 2048 or higher

You see both Primary key (Primary = checked) and subkey (Primary = unchecked)



4.4. From the below window, click Export.



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. 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.

The screenshot shows a window titled "Export - Kleopatra" with a close button in the top right corner. The main area contains a PGP public key block. The text is as follows:

```

-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: User-ID: Example Name <example_email@company.com>
Comment: Valid from: 3/1/2024 9:36 AM
Comment: Valid until: 3/1/2027 12:00 PM
Comment: Type: 2,048-bit RSA (secret key available)
Comment: Usage: Signing, Encryption, Certifying User-IDs
Comment: Fingerprint: 410699BCD4FE30FA345E20865C540FBF221257DA

mQENBGXh9eEBCADNBEONK6PGFQbBv2W6cIKJg+esH3JlzGWSNKb4CnWmlwVv2M0
XMtmVu6JuiFc600TLRrR5CSIy5auPzfDi+fEcT72ePfcBRM8yePk8TDDhGxIH4G
+g0IoQqnm6D4l7qelm6/CywWSIeZ6GV/P47L9Cjx6kZqJwVaSgGdtMS386AdFfyj
hHC9DLuH9//pZDbBxMHilOP2ix2BQvtz9XzrjwM2r20eW2gWg+L/em19JNLcjhv9
H8P7JNHIRaZhdsQUSu35jTZlfi5XaxZ+NxI/olQvQdKXhHnAYHfMNPkAFfe7npaJ
9e6gULWEcoGQlIXc6g74RafYECh/2s2Zc79LABEBAAG0KEV4YW1wbGUgTmFtZSA8
ZXhhbXBsZV9lbWVpY291bnRlY291bnRlY291bnRlY291bnRlY291bnRlY291bnRl
IIZcVA+/IhJX2gUCZeH14QIbAwUJBaO8PwULCQgHAgIiAgYVCgkICwIEFgIDAQIe
BwIXgAAKCRBcVA+/IhJX2gQpB/9IGWn45Qfk/3JiAzAaAOGfjWewXM80bBII64kx
n8aVc3KdlrFRmTVck7WF2n4jmTp/IERztzUIPO4J5fwPG2FKvL8lDtXh6SQc6Gic
/5iconCB9K07cPa59GQE5PmGl7I8vp4FhC6s2V1jaXhqu4HR5IKfIXwsguEvkh4E
JfMigauSbTxcqyjekwSskZjZpkA6/NciRBRlh4ePCTfA9vR+zKLaJRjZ5jWr9GJu
WMN7+Oso7dnLgMYWO07m2vT/QVlrHodDrRXDpvetm4mK/X0ngl4Yp17WQBH290oh
Br4CELFQWSYrnOFz13pGzvxmXjrNMcuZ3es5gaECglavy3vCuQENBGXh9eEBCACr
5UVxB5Wo/kxrFaCXPbgA4Br5oMa8pmfI3d7BpxUkM1fyNbObogI25P/NO3Uxhk9D
miKz3e5AHsI1xglp10tCyRJNvKcwGFIum4PjbbZrSulxfePhd+YaU0I1ycvswSbd
qWfmWNuTo7E2NvfTx7UXMpwPbYQBZsBepdJTBFWshVBh0p1tj6hnt2mCTc15a3yd
+sKVXrK4OLZoJOJnlHxLt+3+CVGIjoUE6RcvZv4tG+DV4Izv7ROK30giFQvVzGyJ
zXiWC+qqLGorWulprtnj05/LDQHXyzrWGs45wpAZjtJlFBR6RTONFk7HJ+ittk
idpSFDk5HdDrHoYpFjNHABEBAAGJATsEGAEIACYWIQRBBpm81P4w+jReIIZcVA+/
IhJX2gUCZeH14QIbDAUJBaO8PwAKCRBcVA+/IhJX2nwpB/jnYGH3mi4izI1qN/Tk
M1Q6ahwT5DoQ3qImG+NHZ+G19hezaYhW+/JLFoiNO/09W1zFvAN3aFA7aZpVWR8
NI27b+XksGm2Q2ZmkTGmq5cSMb7sPfb557T7g19JWjDqmPQ1jz9/PMYz63pAKaF
6kPVEoR2iKGhLTbnBoTfbfknREvm3XdHdwZGUj+ABKzA+HtIH5M+c7UnGGkxdjTe
8HRNn529K5B0i5ris8MpZwnlh41o2XQ8Kf2mP2S1myX0qezQCgteZ8tv6jLxjcdk
y9taJGwQHAs5fSGLYUYygwxkbCgYA4cpVKuyE2aRokwYTKB9OmMnKyWpQ//cRPaR
Cao=
=Vofv
-----END PGP PUBLIC KEY BLOCK-----
    
```

At the bottom right of the dialog box, there is a "Close" button.

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.

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

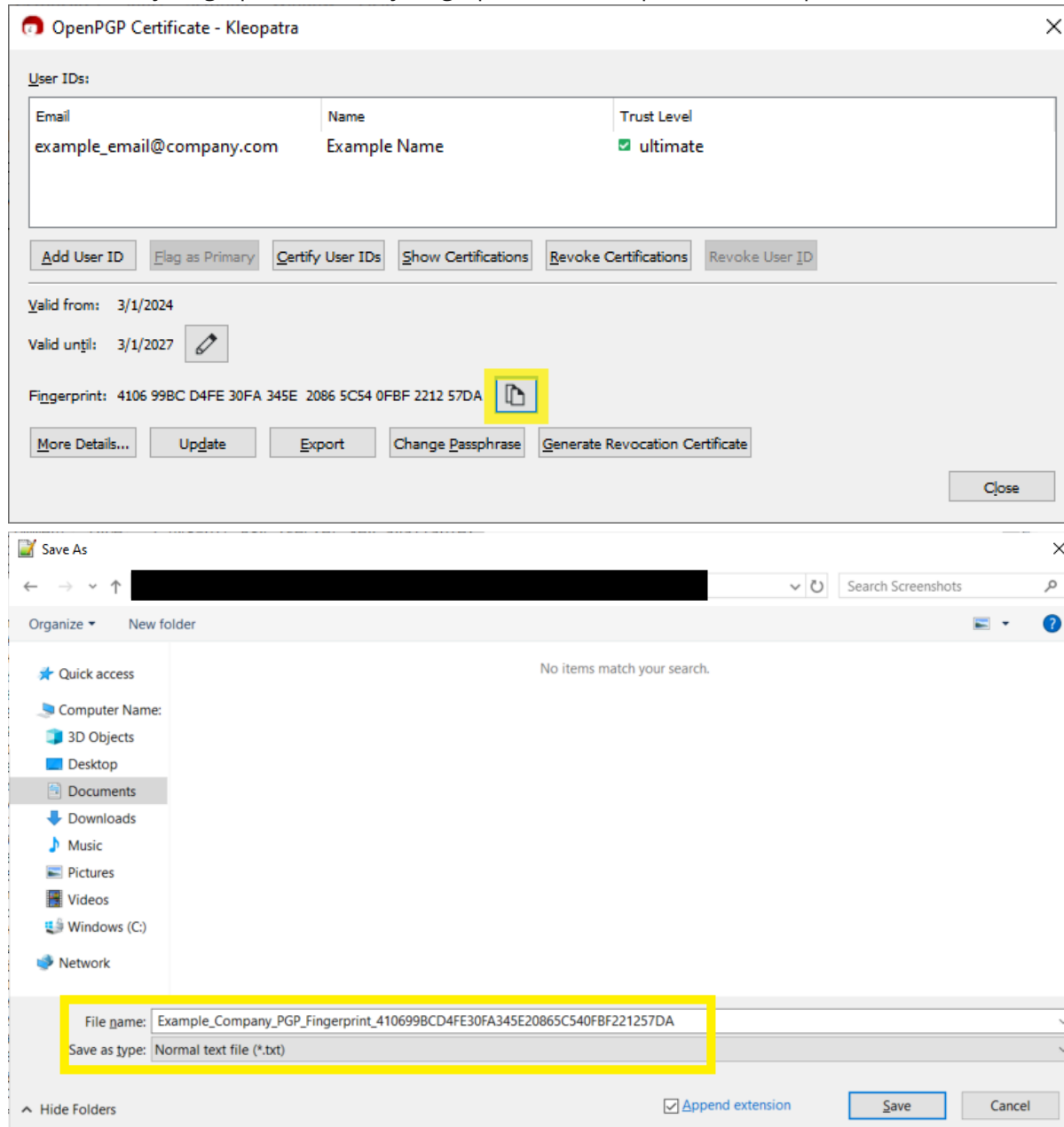
```

1 -----BEGIN PGP PUBLIC KEY BLOCK-----
2 Comment: User-ID: Example Name <example_email@company.com>
3 Comment: Valid from: 3/1/2024 9:36 AM
4 Comment: Valid until: 3/1/2027 12:00 PM
5 Comment: Type: 2,048-bit RSA (secret key available)
6 Comment: Usage: Signing, Encryption, Certifying User-IDs
7 Comment: Fingerprint: 410699BCD4FE30FA345E20865C540FBF221257DA
8
9
10 mQENBGXh9eEBCADNBEONKg6PGFQbBv2W6cIKJg+esH3JLzGWSNkb4CnWmlwVv2M0
11 XMtmVu6JuiFc600TLRrR5CSiy5auPzfdi+fEcT72ePfcMBRM8yePk8TTDhGxIH4G
12 +g0IoQqnm6D4l7qelm6/CywWSIeZ6GV/P47L9Cjx6kZqJwVaSgdtMS386AdFfyj
13 hHC9DLuH9//pZDbBxMHILOP2ix2BQvtz9XzrjwM2r20eW2gWg+L/em19JNLcjhv9
14 H8P7JNHIRaZhdsQUSu35jTz1fI5XaxZ+NxI/olQvQdKXhNAYHfMNPkAFfe7npaJ
15 9e6gULWecQq1IXc6g74RafYECh/2s2Zc79LABEBAAG0KEV4Yw1wbGUgTmFtZSA8
16 ZXhhbXBsZV9lbWVpYEBjY21wYW55LmNvbT6JAVcEEwEIAEewIQRBbpm81P4w+jRe
17 IIZcVA+/IhJX2gUCZeH14QIbAwUBaO8PwULCQgHAgiIAGYVCgkICwIEFgIDAQIE
18 BwIXgAAKRCBcVA+/IhJX2gQpB/9IGWm45Qfk/3JiAzAaAGGfjWewXM80bBII64kx
19 n8AvC3kdlrFRmTVck7WF2n4jmTp/IERztzUIPO4J5fwPG2FKvL81DtXh6SQC6GIC
20 /SiconCB9R07cPa59GQE5PmG17I8vp4FhC6s2V1jaXhqu4HR5IKfIXwsguEvkh4E
21 JfMigauSbTxcqyjekwSskZjZpkA6/NciRBRLh4ePCTfA9vR+zKLaJRjz5jWr9GJu
22 WMN7+Oso7dnLgMYW007m2vT/QVlrHodDrRXDpvecm4mK/X0ng14Yp17WQBH290oh
23 Br4CELFQWSYrnOFZ13pGzvxmXjrnMcuZ3es5gaECglavy3vCuQENBGXh9eEBCACR
24 5UVxB5wo/kxrFaCXpBgA4Br5oMa8pmfI3d7BpxUkM1fyNbObogI25F/NO3Uxhk9D
25 miKz3e5AHSI1xglp10tCyRJNvKcWGFium4FjbBzrSulxfePhd+YaUO1IycvswSbd
26 qWfmWNuotoE2Nvftx7UXMpwPbYQBZsBepdJTBFWshVBhOp1tj6hnt2mCtcl5a3yd
27 +sKVXrK4OLZJoJnlHxLt+3+CVGIjoUE6RcvZv4tG+DV4Izv7ROK30giFQvVzgyJ
28 zXiWc+qLgorWulprtnj05/LDGQHxyzrWGs45wpA2jtJlFBR6RTONFk7HJ+ittk
29 idpSFDk5HdDrHoYpFjNHABEBAAGJATsEGAEIACYWIQRBBpm81P4w+jReIIZcVA+/
30 IhJX2gUCZeH14QIbDAUJBAO8PwAKRCBcVA+/IhJX2nwpB/jnYGH3mi4izI1qN/Tk
31 MIQ6ahwT5DoQ3qImG+NHZ+G19hezaYhW+/JLFoiNO/09W1ZFvAN3aFA7aNZpVWr8
32 NI27h+XksGm2Q2ZmkTGmq5cSmb7sPfb557T7g19JWjDgmPQ1jz9/PMYzM63pAKaF
33 6kPVEoR2iKGhLTbnBoTfbfknREvm3XdHdwZGUj+ABKzA+HtIH5M+c7UngGkxdjTe
34 8HRnN529K5B015riS8MpZwm1h41o2XQ8KfZmP2S1myX0qezQCgteZ8tv6jLxjcdK
35 y9taJGWQHAs5fSGLYUYygwxkbCgYA4cpVKuyE2aRokwYTKB9OmMnKyWpQ//cRPaR
36 Cao=
37 =VOfv
38 -----END PGP PUBLIC KEY BLOCK-----
39

```

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.



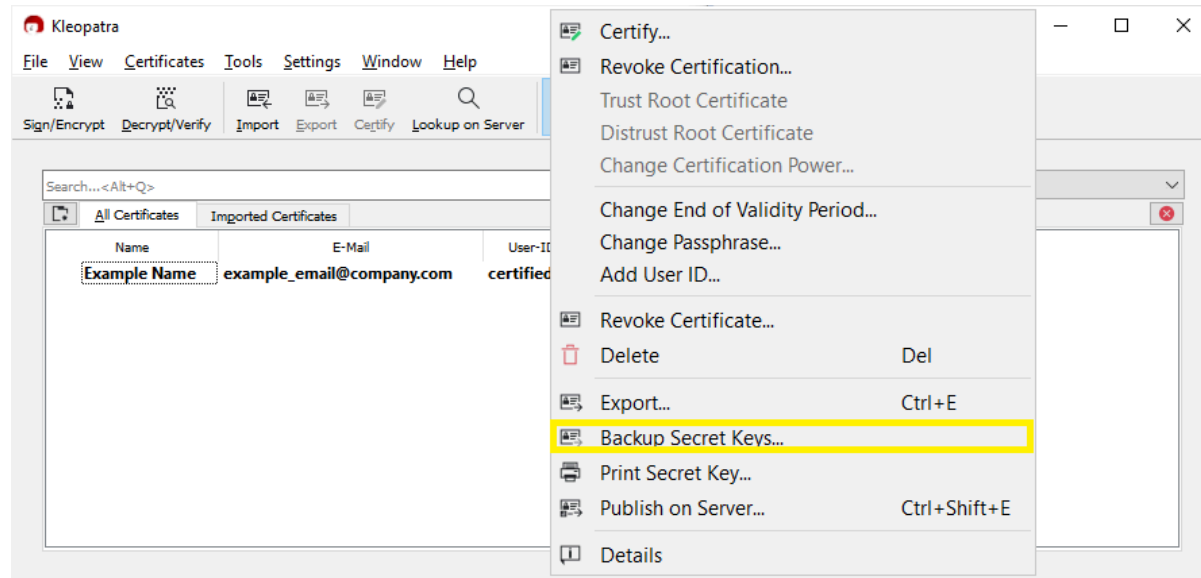
- 4.8. Forward the key to your Equifax MFT point of contact as an email attachment.

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.

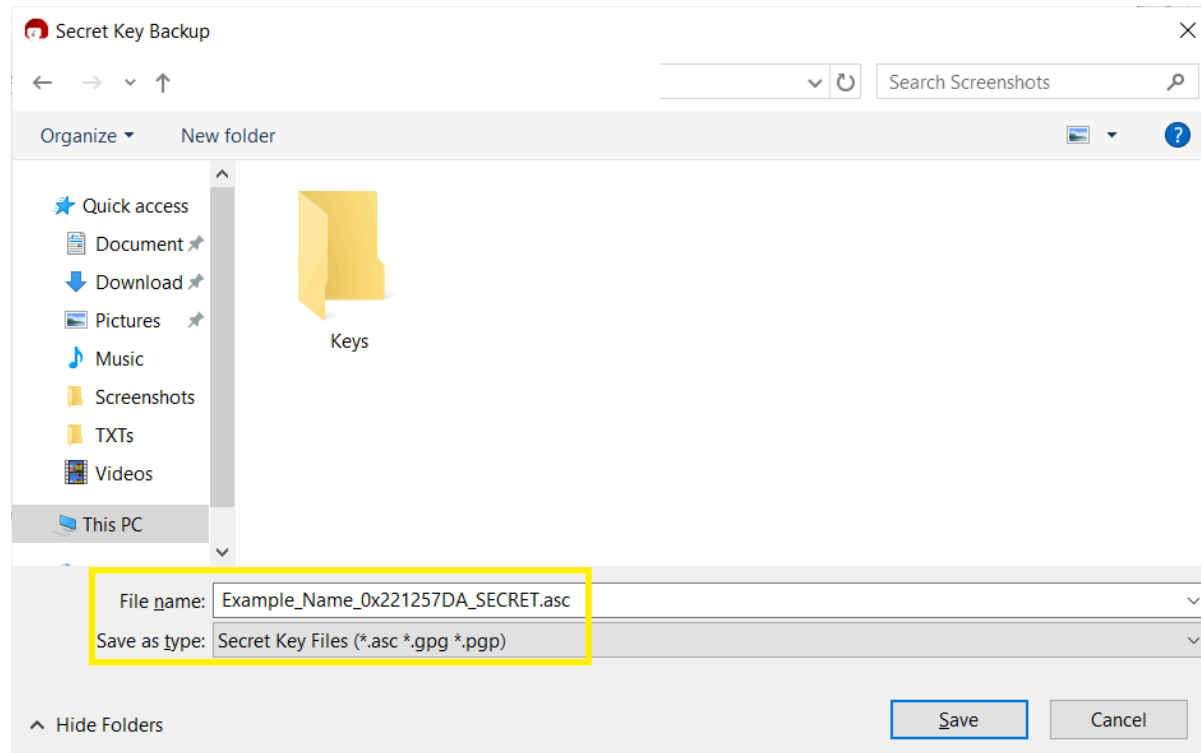
5. Exporting and Backing Up Private Key

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...



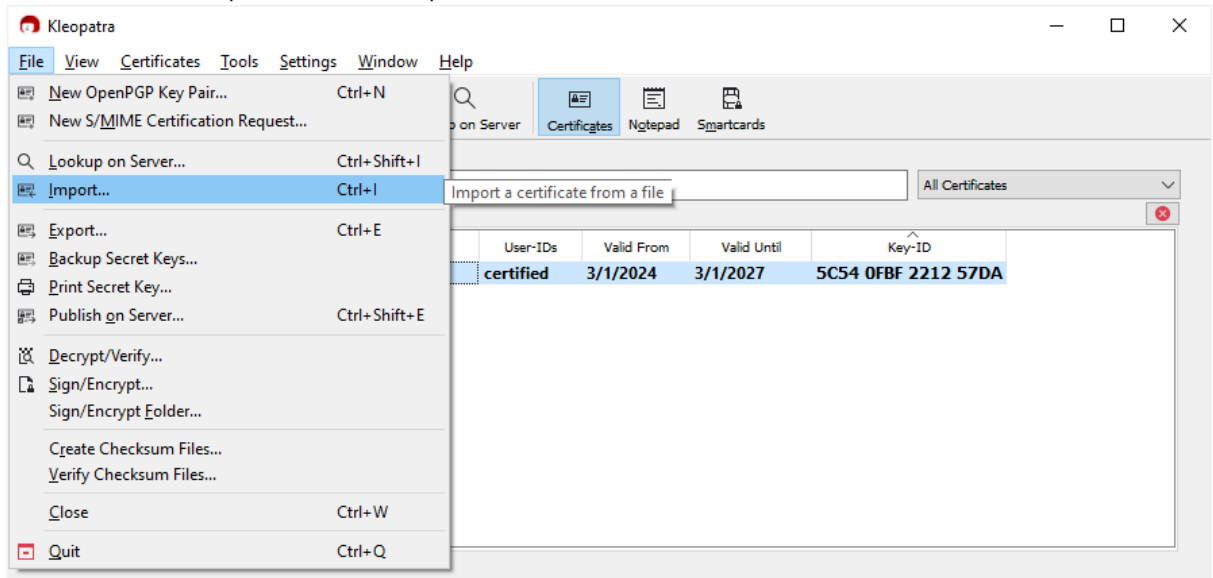
- 5.2. Click the folder icon, then choose file name and saving location.



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

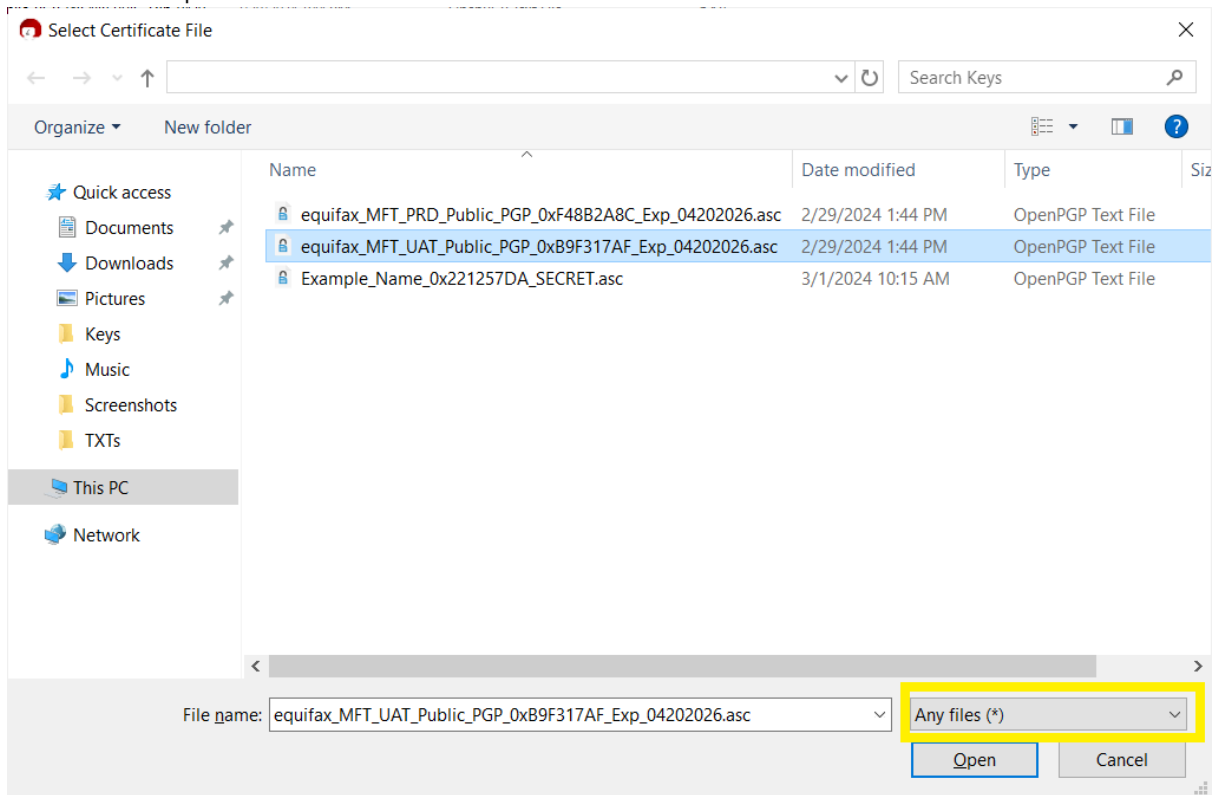
- 6.1. To send Equifax an encrypted file, you must import and certify both the Equifax SFG UAT PGP Key and SFG PRD PGP Key. Equifax should provide you the keys as email attachments. Download both keys from your email and save on your local drive.
- 6.2. Go to Kleopatra File Import...



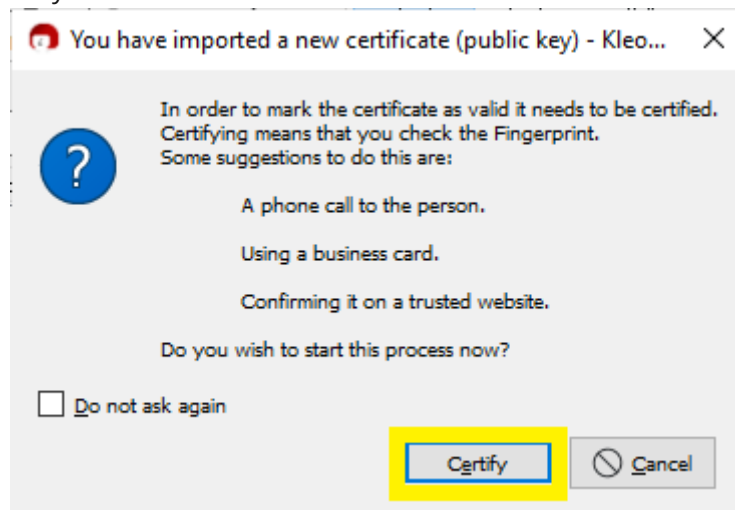
- 6.3. Go to the directory where you saved the keys and select them. Change the file type to any type in order to view the keys.

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. Click Open.

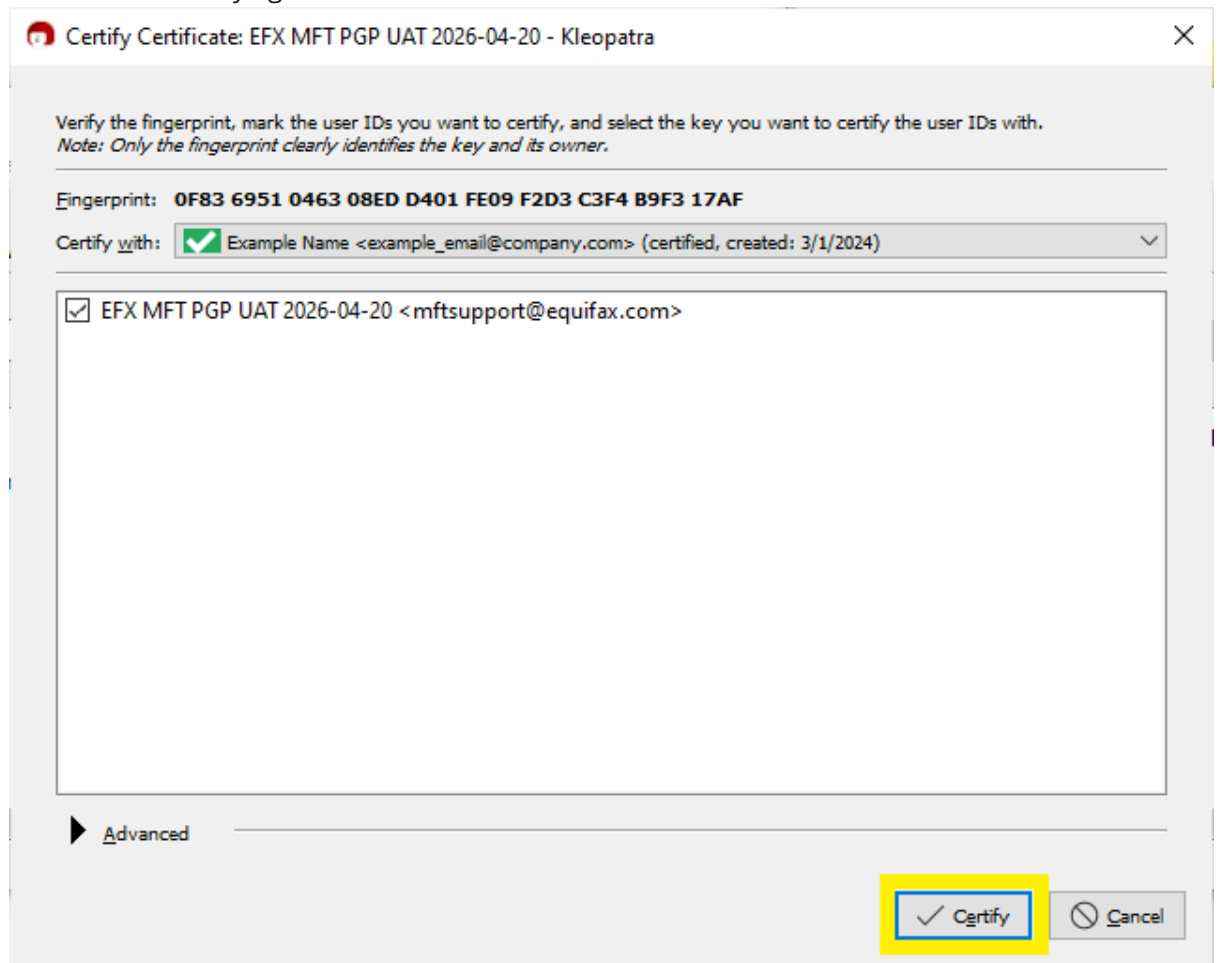


6.5. Click Certify.



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.

6.6. Click Certify again.

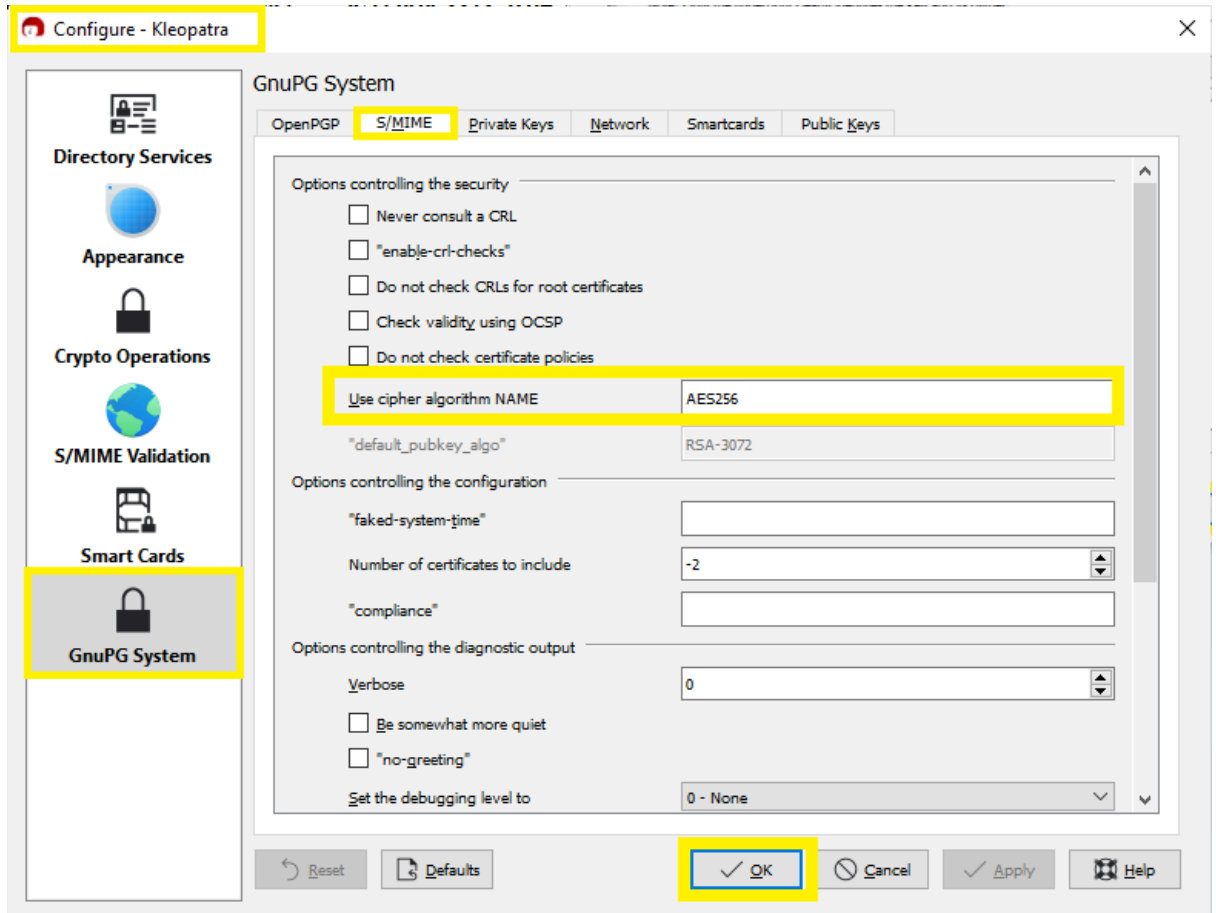


6.7. Repeat steps 6.1 - 6.5 as needed.

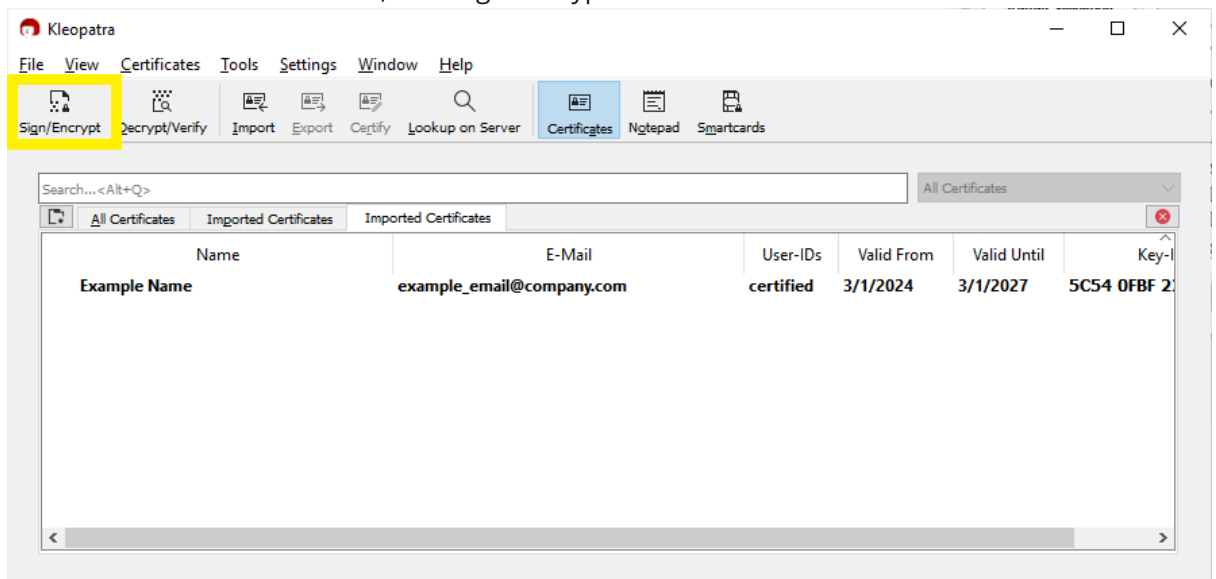
IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

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.

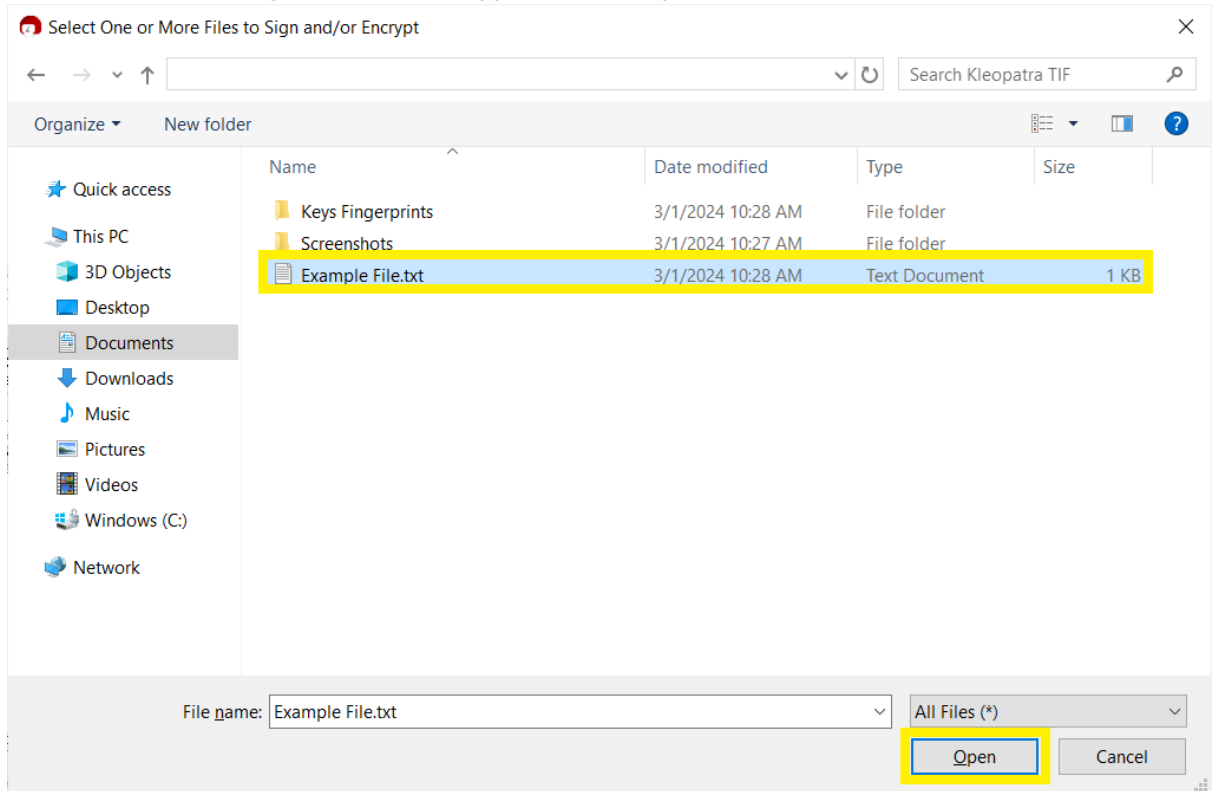


- 7.2. From the home screen, click Sign/Encrypt...



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.

7.3. 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.

Sign/Encrypt Files - Kleopatra

Sign / Encrypt Files

Prove authenticity (sign)

Sign as: Example Name <example_email@company.com> (certified, created: 3/1/2024)

Encrypt

Encrypt for me: Example Name <example_email@company.com> (certified, created: 3/1/2024)

Encrypt for others: Please enter a name or email address...

Encrypt with password. Anyone you share the password with can read the data.

Output

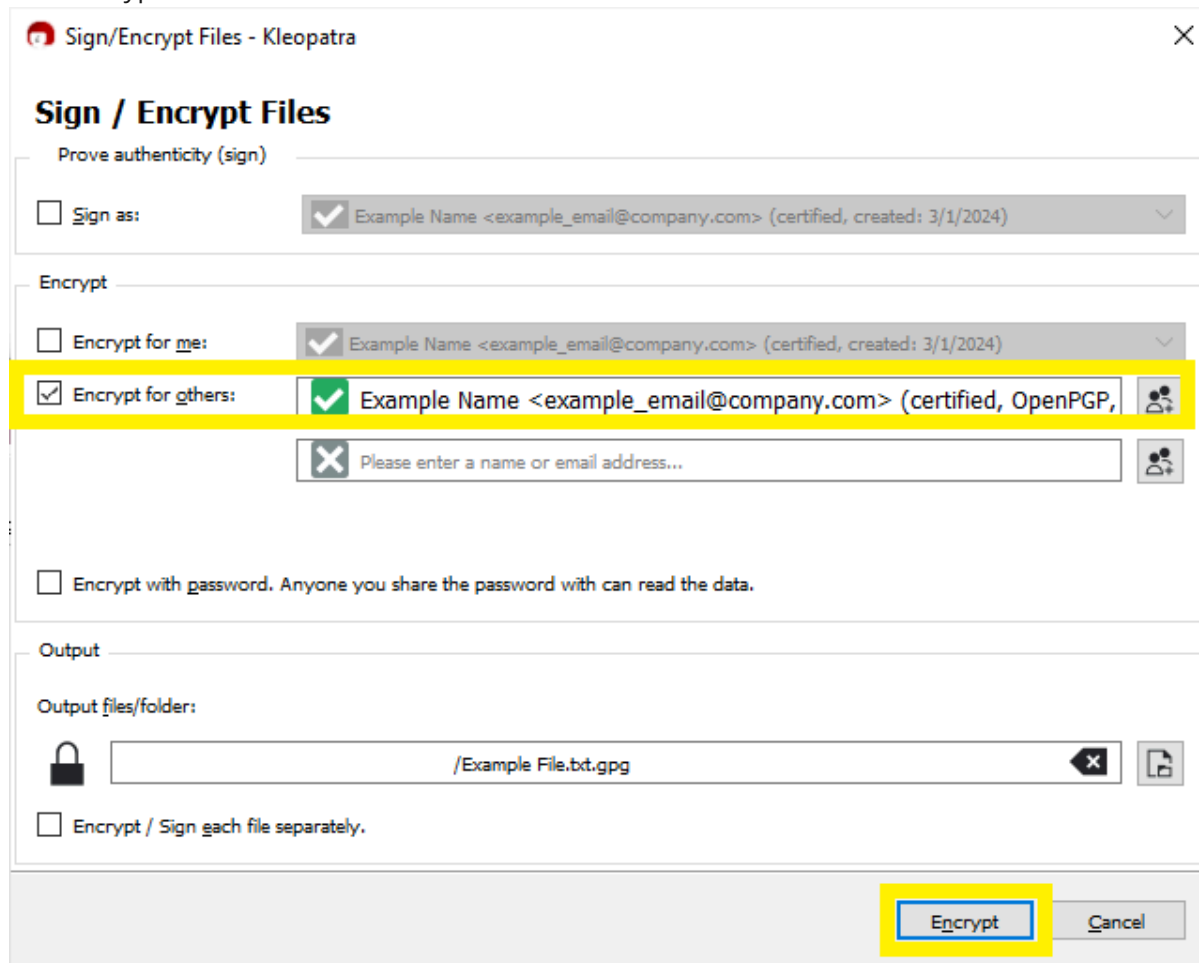
Please select an action.

Encrypt / Sign each file separately.

Next Cancel

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.

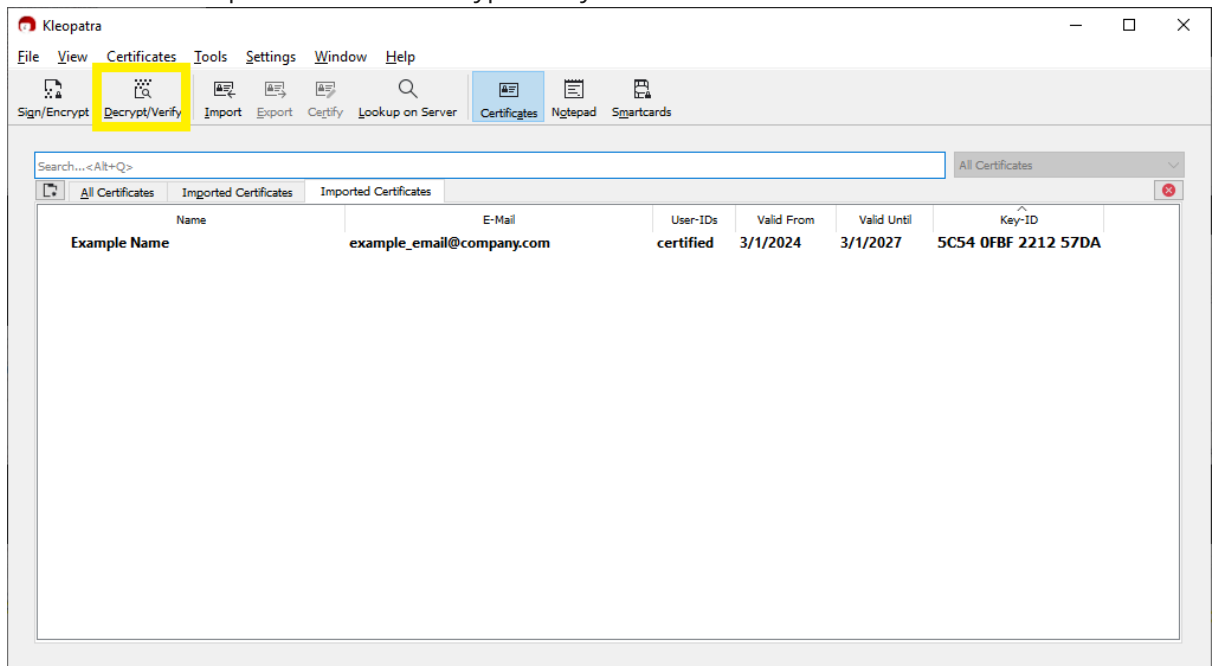
7.5. Click Encrypt.



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.

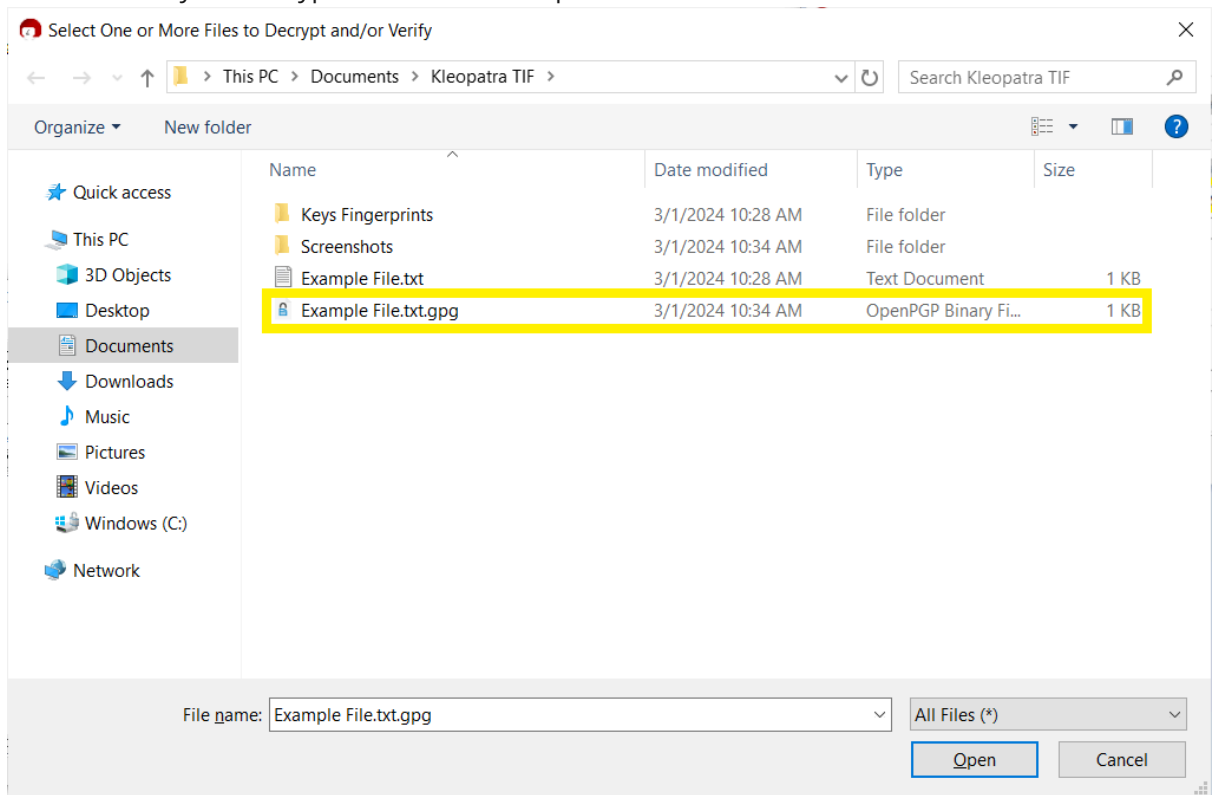
8. Decrypting Files Sent from Equifax

- 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...



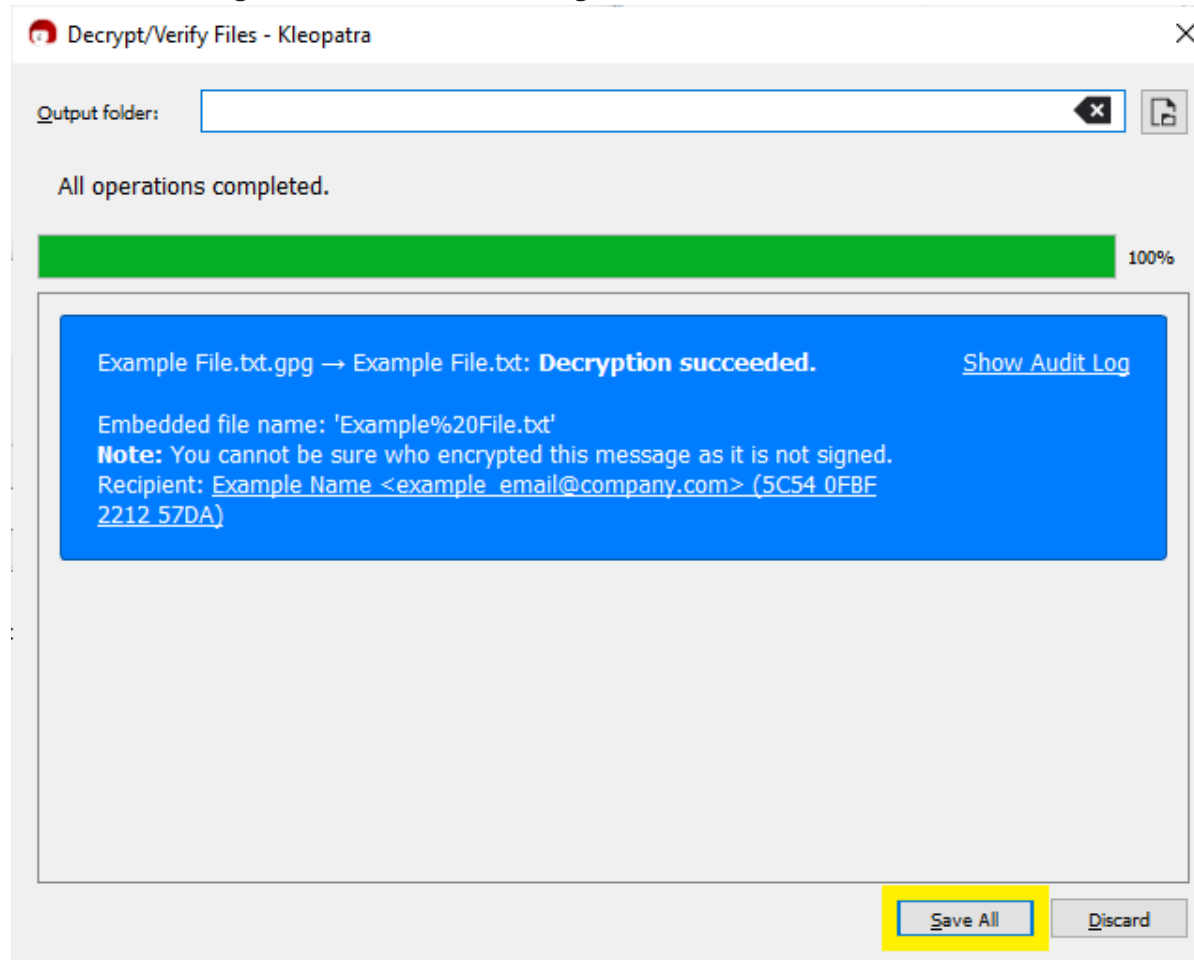
IMPORTANT NOTE: Equifax does not recommend any specific File Encryption Software. We do suggest, however, that you choose a software package that has its own help desk so that you may receive support if you encounter any issues while using the software.

8.3. Select your encrypted file 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.

- 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.