

# 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

## **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

## 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.

### 2. Installation

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

Installer	Language	×			
-	Please choose a language for the setup. Bitte die Sprache des Installations-Vorgangs angeben.				
	English	~			
	OK Cancel				

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

🔒 Gpg4win Setup		- 🗆 X				
Gpg4win	Choose Components Choose which features of Gpg4win you want to install.					
	Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.					
Select components to inst	all: CouPG CouPG GpgQL GpgQX Browser integration	Description Position your mouse over a component to see its description,				
Space required: 84.9 MB						
Gpg4win-4,1,0						
	< Back	Next > Cancel				

2.3. Click Next> then click Install.

🔒 Gpg4win Setup			-		×
Gpg4win	Choose Install Locat Choose the folder in wi		win.		
	n the following folder. To i Click Install to start the in		folder, cli	ck Browse	
Destination Folder	))Gpg4win		Brow	se	
Space required: 101.0MB Space available: 586.4GB					
og4win-3.1.8		< <u>B</u> ack <u>I</u> ns	tall	Cance	ł

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



## 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  $\rightarrow$  New OpenPGP Key Pair...



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

7 Create OpenPGP Certificate - Kleopatra ? X					
Enter a name and/or an email address to use for the certificate.					
Name					
Example Name					
Email address					
example_email@company.com					
Protect the generated key with a passphrase.					
Advanced Settings					
OK Cancel					

3.3. Click Advanced Settings.

	$\sim$		-	-	
闭 Create Oper	PGP Certificate - K	leopatra	?	$\times$	
Enter a nam	ne and/or an en te	nail addres	ss to use	for	
Name					
Example Na	ame				
Email address					
example_e	mail@company	.com			
Protect t	he generated k	ey with a	passphra	se.	
		Advan	ced Setti	ngs	
	(	ОК	Cano	el	

IMPORTANT NOTE: Equifax does not recommend any specific File

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

🕡 Advanced Settings - Kleop	atra	?	×
Technical Details			
Key Material			^
• RSA	2,048 bits	~	
✓ + RSA	2,048 bits	~	
○ DSA	2,048 bits	$\sim$	
+ Elgamal	2,048 bits	~	
O ECDSA/EdDSA	ed25519	$\sim$	
+ ECDH	cv25519	~	
Certificate Usage			
✓ Signing	Certificatio	n	
Encryption	Authentica	tion	н.
✓ Valid until: 3/	2/2025	$\sim$	~
	OK	Cancel	

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.

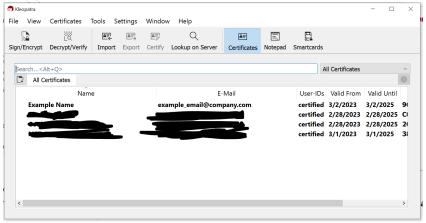
🕡 Advanced Settings - Kleop	🕡 Advanced Settings - Kleopatra ?		
Technical Details			
Key Material		^	
• RSA	2,048 bits ~		
✓ + RSA	2,048 bits ~		
O DSA	2,048 bits		
+ Elgamal	2,048 bits		
O ECDSA/EdDSA	ed25519 ×		
+ ECDH	cv25519 ×		
Certificate Usage			
Signing	Certification		
Encryption	Authentication		
Valid until: 3/	<mark>2/2025</mark> ~	~	
	OK Can	cel	

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

					?	$\times$
÷	Key Pair Crea	ation Wizard				
Key	Pair Successf	ully Created	I			
step	r new key pair was o s below.	reated successfully	. Please find detail	s on the result and s	iome suggeste	d next
	Key pair created succ Fingerprint: A70541A		900FF7CB523C32	SA0		
Ne	ext Steps					
		Make a Ba	ickup Of Your Ke	y Pair		
		Send	Public Key By EM	el		
		Upload Public	: Key To Director	/ Service		
				Finish	Can	cel

## 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....

👦 OpenPGP Certificate - Kleopatra			? ×
User IDs:			
Email	Name	Trust Level	
example_email@company.com	Example Name	ultimate	
Add User ID Flag as Primary Certif	User IDs Show Certifications	Revoke Certifications Revoke User ID	
Valid from: 3/2/2023			
Valid until: 3/2/2025 🖉			
Fingerprint: 2B08 835D FA27 9AF4 7134	57C3 9C63 0524 824A CF3E		
More Details Update Ex	Change Passphrase Ger	nerate Revocation Certificate	
			Close

- 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 =



IMPORTANT NOTE: Equifax does not recommend any specific File

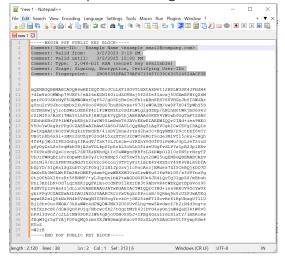
4.4. From the below window, click Export.

OpenPGP Certificate - Kleopatra Jser IDs:			
Email	Name	Trust Level	
example_email@company.com	Example Name	ultimate	
Add User ID Flag as Primary C	ertify User IDs Show Certificat	ions Revoke Certifications Revoke User ID	
alid from: 3/2/2023 alid until: 3/2/2025			
ingerprint: 2B08 835D FA27 9AF4 7	134 57C3 9C63 0524 824A CF3	E	
More Details Update	Export Change Passphras	Generate Revocation Certificate	
	change rasspiras	denerate Revocation certificate	Close

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.

<pre>LBit State State Model</pre>
Close

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



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.

OpenPGP Certificate - Kleopatra					?	$\times$
User IDs:						
Email	Name	Trust Level				
example_email@company.com	Example Name	ultimate				
Add User ID Flag as Primary C	Certify User IDs Show Certifications	Revoke Certifications	Revoke	User ID		
Valid from: 3/2/2023						
Valid until: 3/2/2025						
Fingerprint: 2B08 835D FA27 9AF4 7	7134 57C3 9C63 0524 824A CF3E					
More Details Update	Export Change Passphrase	Generate Revocation Certi	ficate			
					Close	e
			-	*::::::::::::::::::::::::::::::::::::::		
📓 Save As						×
$\leftarrow \rightarrow \checkmark \uparrow \square >$ Computer	Name: ATL100000843159 > Deskt	op 🗸	U	✓ Search Deskto	р	
Organize • New folder					•	?
Desktop ^ Nar	ne	Date modifi	ed	Туре		Siz
	The second se		MICE	Text Docur		
V Scomputer Name:				Text Docur Text Docur		
> 3D Objects			-			
> Desktop						
> 🗟 Documents						
<ul> <li>         Downloads     </li> <li>         Music     </li> </ul>						
> Fictures						
> 📑 Videos						
> 🔩 Windows (C:)						>
	npany_PGP_Fingerprint_2B08835DFA	279AF4713457C39C63052	4824ACF	3E		~
Save as type: Normal text f						~
▲ Hide Folders		Append extension		Save	Cancel	

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

## 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.

👩 Backup Secret Key								×
← → + ↑	> This	PC > Desktop	v	0	P See Set			
Organize • Ner	w folder					E	- (	0
E Documents	* * *	Name Diquifux Segmentation_Ox08614E35_public (Quase Segn		1/14/	notified 2021 5:06 PM 2020 9:00 AM		Type ASC file File fold	
	¥ 6							3
File name:	Geoffre	y Lewis_0x23C328A0_SECRET.asc						v
Save in type:	Secret R	ley Files (*.exc *.gog *.pgp1)						~
∧ Hide folders					Save	<	Cancel	Ξ,

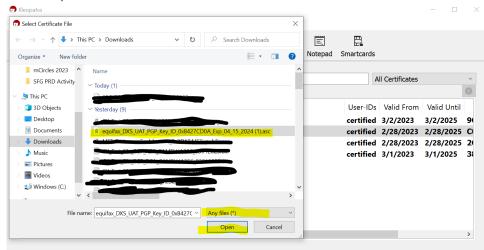
## 6. Importing a Public Key

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...

						in since				
C Respeters									- 0	3
He Nor Cetholas	Tools Settings	Window	Nep							
<ol> <li>Nor Key Palue</li> </ol>	Col-45	<u>k</u> – 2	¢	Q,	8		-			
9. Lookspronderman	04-080-1	a. au	6- 14	dag or bever-	Calification	Rotope	, Statist	<b>b</b>		
Ri Import	CM-F									_
R. Supet.	CM-E							el Continuino		10
81 Raday Secret Keys-				P Mail			Dar-Da	States Report	The loss	
(2) Print Secret News			il ingles	elefter på han av			urrilled	2/11/2011	2,02,260	-
St. Publish on Server.	CM-CMP-E									
S. Despatients.										
G Spyllaget-										
Sep. Energeti folder										
Center Decknere Files.	_									
Velly Checkpury Rep.										
Case	Calvat									
10 Gel	0440									- 2
		-	1	17 195	10	- 0.	C 900	eyounav	eacque	1927

- 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.



6.5. Click Certify.



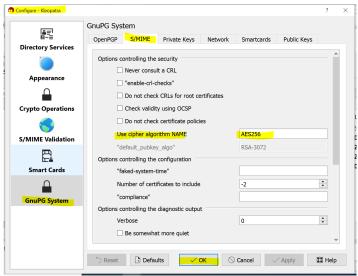
#### 6.6. Click Certify again.

,	e: Equifax MFT UAT PGP Key Expires 04-15-2024 mftsupport@equifax.com - Kleopatra	
	gerprint, mark the user IDs you want to certify, and select the key you want to certify the user IDs with. he fingerprint clearly identifies the key and its owner.	
ingerprint:	10DC B47D 20C2 2F4E 46AD 27E8 8468 2D6E B427 CD0A	
ertify with:	(certified, created: 2/28/2023)	~
✓ Equifax	MFT UAT PGP Key Expires 04-15-2024 mftsupport@equifax.com	
Advance	d	
		ancel

6.7. Repeat steps 6.1 - 6.5 as needed.

## 7. Encrypting Files Sent to Equifax

7.1. Go to Settings  $\rightarrow$  Configure Kleopatra  $\rightarrow$  GnuPG System  $\rightarrow$  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....

Verify Import Ex	port Certify L	Q Lookup on Server	E Certificates	E E	All Certificates		~
Name AT PGP Key Expires 0-		E			All Certificates		~
Name AT PGP Key Expires 0-		F-I					100
Name AT PGP Key Expires 04		E.I					0
			Mail	User-ID:	Valid From	Valid Until	
	4-15-2			certified	2/3/2022	4/15/2024	84
e	exam	nple_email@comp	pany.com	certified	3/2/2023	3/2/2025	9(
					2/28/2023		
				certified	3/1/2023	3/1/2025	31
					certified		certified 2/28/2023 2/28/2025

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

> -> -> -> ->	i > This	PC > Documents	~	U	Q 503	rch Docume	oto		Ē
	· · · · · · · ·	re > bocaments	*	0	/~ 3ea	ich Docume	ints		
Organize 🔹 🛛 N	lew folder					-		0	Notepad
📌 Quick access	^	Name	^			Date modifie	ed		
Documents	*					2/8/2023 9:2	3 AM		
						2/6/2023 9:0	4 AM		
Downloads		-				2/23/2023 3	:15 PM		
Pictures	*	A Carlo Martin				1/6/2023 10	21 AM		
<u>~</u>	-9		-			1/6/2023 1:4	19 PM		
Desktop		ExampleCompany	_Tst_File.txt		1	2/24/2023 1	1:35 AM		
	-								
	<b>Ann</b> y								
This PC									
🧊 3D Objects									
E. Desktop	v .	<						>	
	File nam	ne: ExampleCompany_Ts	st_File.txt	~	All Files (*	)		~	

IMPORTANT NOTE: Equifax does not recommend any specific File

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.

	eopatra	?
Sign / Encry	/pt Files	
Prove authenticity	(sign)	
Sign as:	Continue of the second	
ncrypt		
Encrypt for me:	(certified, created: 3/1/2023)	
Encrypt for othe	rs: 🔀 Please enter a name or email address	
Encrypt with pa	ssword. Anyone you share the password with can read the data.	
	ssword. Anyone you share the password with can read the data.	
] Encrypt with pa: Dutput		
Dutput Please select an ac	tion.	
Dutput Please select an ac		
output lease select an ac	tion. ach file separately.	ance

#### 7.5. Click Encrypt.

E	🙃 Sign/Encrypt Files - Kleopatra		? ×
bg	Sign / Encrypt Files		
21/	Prove authenticity (sign)		
	Sign as:	Customer Enablement <mft.project@equifax.com> (certified, created: 3/1/2023)</mft.project@equifax.com>	$\sim$
YF	Encrypt		
_	Encrypt for me:      MFT	Customer Enablement <mft.project@equifax.com> (certified, created: 3/1/2023)</mft.project@equifax.com>	~
 All	Encrypt for others: 🛃 Equ	ifax MFT UAT PGP Key Expires 04-15-2024 mftsupport@equifax.com (certified, Op	enP( 😤
-	X Plea	ase enter a name or email address	•••
u			
a			
30 30			
F			
	Encrypt with password. Anyone	e you share the password with can read the data.	
	Output		
	Output files/folder:		
	G, (aul 20/Document	ts/ExampleCompany_Tst_File.txt.pgp	
	Encrypt / Sign each file separa	telv	
	energie orgin cucir nie sepuru		
		Encrypt	Cancel

## 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...

👦 Kleopatra										- 0	>
File View	Certificates	Tools Se	ettings Wi	ndow I	Help						
Sign/Encrypt	Decrypt/Veri	ify Import		rtify Loc	Q okup on Server	a≡ Certificates	E. Notepad	E Smartcards			
Search <a< td=""><td>Alt+Q&gt;</td><td></td><td></td><td></td><td></td><td></td><td></td><td>ł</td><td>All Certificates</td><td></td><td>~</td></a<>	Alt+Q>							ł	All Certificates		~
🗔 All G	ertificates										$\otimes$
	N	ame			E-	Mail		User-IDs	Valid From	Valid Until	
Equifa	x MFT UAT P	GP Key Expire	es 04-15-2					certified	2/3/2022	4/15/2024	8∠
	ple Name			examp	le_email@com	oany.com			3/2/2023	3/2/2025	91
Geon	- Lowis								2/28/2023 2/28/2023	2/28/2025 2/28/2025	
		a history and		-					3/1/2023	3/1/2025	31
									• •		
<											>

8.3. Select your encrypted file and click Open.

7 Select One or More Files to Decrypt and/or Verify	$\times$
$\neg \leftarrow \rightarrow \checkmark \uparrow$ $\textcircled{B}$ > This PC > Documents $\checkmark$ $\textcircled{V}$ Search Documents	
Organize • New folder	?
Name Date modified	
2/8/2023 9:23 AM	
<b>S This PC</b> 2/6/2023 9:04 AM	
<b>3D Objects</b> 2/23/2023 3:15 PM	
Desktop	
Documents	
↓ Downloads	
h Music	
Pictures	
📲 Videos	
🐛 Windows (C:)	
v <	>
File name: ExampleCompany_Tst_File.txt  V All Files (*) Open Cancel	~

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.

•	Decrypt/Verify Files - Kleopatra	? ×
Output folder:	C:/Users/jacquita.davenport/Desktop	•
All operations	s completed.	
		100%
mailbox-2	2018-03-13-15-21-13.64845.zjp.pgp → mailbox-2018-03-13-15-21-13.64845.zjp: <b>Decryption</b>	
succeed	led.	
Note: Yo	u cannot be sure who encrypted this message as it is not signed.	
$( \bigcirc )$		
	Save All	Discard

IMPORTANT NOTE: Equifax does not recommend any specific File