

Intro to PGP Encryption & SFTP – Live Demo Recap

On May 14, 2025, Onpoint held a webinar for submitters to the Health Care Payments Data (HPD) program that reviewed the file encryption and secure submission process. This document provides an overview of the process.

Getting Started

If an organization does not already have PGP or SFTP applications installed, we recommend GPG4Win (which includes Kleopatra, see the logos on the bottom left) for PGP key management, encryption, and decryption. We recommend WinSCP (see below right) as an SFTP client. Onpoint will try to provide support for any tools that you choose but we have extensive experience with these recommended tools.



Creating a PGP Pair

To create a new PGP key pair, open Kleopatra and select New OpenPGP Key Pair from the File Menu.



Enter a name and email address for the key pair. This can be any name and email address. The email address entered will not be used for communication.

You may choose to protect the key with a passphrase. This is not required, but it is recommended for security. If you set a passphrase, you must store it securely for later use. You will need to enter the passphrase whenever you encrypt or decrypt files using the key. The passphrase cannot be recovered or reset. If it is lost or forgotten a new key pair must be generated.

🙃 Kleopatra		-	×
File View Certificates Tools Settings	Vindow Help		
Sign/Encrypt Decrypt/Verify Import Export Certify Looku	Q E E S Certificates Notepad Smartcards Groups		
Welc Kleopa For mo You ca	Create OpenPGP Certificate - Kleop × Enter a name and/or an email address to use for the certificate. Name YourName Email address Email@example.com Photect the generated key with a passphrase. Advanced options Key Material Fra2048 Vald until (between 5/3/2025 and 2/5/2106): 5/2/2028 ✓ OK Cancel		

The "Key Material" used to create the key (located in the bottom half of the screenshot above) must be RSA and a minimum of 2048bits. A higher number will result in more secure encryption but will take slightly longer to generate the key and when you use it to encrypt and decrypt. The options Onpoint accepts are rsa2048, rsa3072, rsa4096.

You have the option to set an expiration date for your key pair. When the key expires it can no longer be used for encryption and a new key must be generated and provided to Onpoint. Expiration is not required but is recommended for security. You can adjust the length of key validity to your preference or organizations policies. If you do not check the **Valid Until** box, the key will remain valid indefinitely.

After adjusting the key settings and clicking **OK**, you will be asked to enter a passphrase for the key if you choose to set one.

🔿 Kleopatra						0-0	×
File View Certificates Too	ls Settings Window	Help					
Sign/Encrypt Decrypt/Venify Import Eq	时 回 Q part Certify Lookup on Server	Certificates Notepad	E Smartcards	Groups			
	Creating Key Pair The process of creating a ke	- Kleopatra pinentry-qt5 Please enter th protect your nr Passphrase: Repeat:	e passphrase t w key ••••••••••••••••••••••••••••••••••••	Cancel	× ire several minutes Cancel		

After entering a passphrase, a pop up will appear showing that a keypair has been created successfully.

In the Kleopatra Certificates pane, you will now see your new keypair listed in bold. The bold text indicates that you hold both the private and public half of this key pair.

e View Certificate	s Tools Set	tings Window	Help							
Encrypt Decrypt/Verify In	nport Export Cer	Q Ify Lookup on Server	Certificates No	E E tepad Smartcards	Sroups					
nter search term <alt+q></alt+q>								All		
All										¢
Name		E	-Mail	Statu	s alid From	alid Uni	Key ID			
YourName		Email@examp	le.com	certif.	. 5/2/	5/2/	C969 1F21			
		14						3		
	Success -	Kleopatra				×				
	A new o	OpenPGP certificate was	created successfull	y.						
	Fingerp	rint of the new certificat	e: 0DCF C818 643C	A60C 66AB 38FE C9	69 1F21 4C72 70)79				
					ОК					

You must export the public half of the key pair from Kleopatra so that you can send it to Onpoint. Right click on your key name and select **Export** from the drop-down menu.

Kleopatra										14	×
e View Certific	cate	es Tools Se E E E E Import Export Ce	ttings Windo	ver Certificates Notepad	Smartcards	Groups					
Enter search term <alt+q< td=""><td>></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>All</td><td></td><td>v</td></alt+q<>	>								All		v
Na	âme			E-Mail	Status	alid Fro	r alid Un	I Key ID			
YourName			Email@exar	mple.com	certif	5/2/	5/2/	C969 1F21	L		
	0	Update Cert	ificates								
	B	Certify									
	1	Revoke Certi	fication								
		Trust Root C	ertificate								
		Change Cert	t Certification Powe	or							
		Disable Certi	ificate								
		Change End Change Pass Add User ID.	of Validity Pe sphrase	riod							
	æ	Revoke Certi	ificate		1.2			die tief			
	Û	Delete		Del	in the						
	3 4	Create Grou	p								
	99	Export	N	Ctrl+E	Export	the selec	ted certif	icate (public	key) to	o a file	
	E ,	Backup Secr	et Keys			-					
	٥	Print Secret	Key								
	盻	Publish on S	erver	Ctrl+Shift+E							
1650	Ø	Details									

Save the key. We strongly recommend including the word "public" in the key name so that you can differentiate it from the private key.

Kleopatra					- 0
Export OpenPGF	P Certificates				×
\leftrightarrow \rightarrow \checkmark 1	🗅 « PGP&SFTP → 2 Send t	o Onpoint - public	~ C	Search 2 Send to	م
Organize • Nev	v folder			≣ •	0
Home Gallery Desktop Documer* Documer*	Name	Date modified No items match	Type Si your search.	ize	
File name: Yo	urPublicKey_public				~
Save as type: Op	enPGP Certificates (*.asc *.gpg *	.pgp)			~
^ Hide Folders				Can	cel

Once the public key has been exported and saved, send it to Onpoint along with your SFTP account registration.

You may also want to export the private half of your PGP key pair. You do not need to do this if you are going to use Kleopatra for encryption and decryption, but you still can if you would like to store a secure back up in another location.

To export the private key, right-click on the key name and select **Backup Secret Keys** from the drop down



Save the private key. We strongly recommend including the word "private" in the key name. A private PGP key should be treated as if it were a password. It should never be shared with anyone (including Onpoint). **Do not send the private half of your PGP key pair to Onpoint.**

Kleopatra					- 0	×
Secret Key Backı	qu				×	
	■ « PGP&SFTP → 2 Keep fo	r yourself - private	~ (Search 2	Keep for P	
Organize • Nev	v folder				≣ • 0	ő
☆ Home	Name	Date modified	Туре	Size		
🔁 Gallery		No items match	your search.			
🛄 Desktop 🖈						
Documer *						
L Downlos +						
File name Yo	urPrivateKeyPGP_SECRET				Ŷ	
Save as type: Sec	cret Key Files (*.asc *.gpg *.pgp)				~	
Hida Foldore				Save	Cancel	
nue rolders				Juve	Curreer	

Importing Onpoint's Public Key into Kleopatra

When you send files to Onpoint you will encrypt them using Onpoint's public key. To do this, you must import the public key you received in the Onpoint welcome email into Kleopatra.

To import the public key, drag and drop it into the **Certificates** pane in Kleopatra.



You will be asked to certify the key you are importing. Certification means that you trust that the key belongs to the person who sent it to you. It is important to take this step after creating your own key because you will use your key to perform the certification.

Select your key name from the Certify with drop down. Click Certify.

🔿 Kleopatra	Certify Certificate: ONPOINT_HEALTH_DATA_PROD - Kleopatra	×		77.5		×
File View Certificates	Verify the fingerprint, mark the user IDs you want to certify, and select the key you want to certify the user IDs with. Note: Only the fingerprint clearly identifies the key and its owner.					
Sign/Encrypt Decrypt/Verify Impt Enter search term <alt+q></alt+q>	Fingerprint: 870F 8656 F324 607E C372 2882 8338 9804 899C E40A Certify with: Image: Certify	v			v	Ð
Al Imported Certificates Name ONPOINT_HEALTH_	ONPOINT_HEALTH_DATA_PROD <support@onpointhealthdata.org></support@onpointhealthdata.org>		39			2
	Advanced Certify	ncel				

If you set a pass phrase for your key pair, you will be asked to enter it.

ncrypt Decrypt/Verify Import Export Certify I	Cookup on Server Certificates Notepad Sm	artcards Groups		
er search term <alt+q></alt+q>			Al	
Name ONPOINT_HEALTH_DATA_PR sup	E-Mail poport@onpointhealthdata.org pinentry-qt5 Please enter the passphrase t YourName <email@example. 2048-bit RSA key, ID C9691F3 created 2025-05-02. Passphrase:</email@example. 	Status alid Froi alid Ur not ce 9/11/ – X a unlock the OpenPGP secret key: com>* 214C727079,	nt Key ID B33B 9804 B9	

Once you have entered your passphrase and successfully certified Onpoint's public key, you should now see Onpoint's key in the Certificates pane.

n Kleopatra				-	×
File View Certificates Tools Sett	ings Window Help				
Sign/Encrypt Decrypt/Verify Import Export Cert	fy Lookup on Server Certificates Notepad	E Smartcards Groups			
Enter search term <alt+q></alt+q>			All		~
All Imported Certificates					٥
Name	E-Mail	Status alid Fror alid Uni	Key ID		
ONPOINT_HEALTH_DATA_PR	support@onpointhealthdata.org	certified 9/11/	B33B 9804 B9		
Tourname	Eman@example.com	cerum. 5/2/ 5/2/			

Notice that it is not in bold text. This is because you have only the public half of the key pair. This means you would not be able to use this key to decrypt.

You now have your key pair set up and Onpoint's public key imported. You are ready to encrypt files.

Encrypting Files Using Kleopatra

To encrypt a file either click **Sign\Encrypt** and select the file you want to encrypt from the File Explorer window. Alternatively, you can simply drag the file(s) you want to encrypt over the Kleopatra window and drop them there, as shown in the image below.

n K	leopatra													-	×
File	View Certif	icates	Tool	s Se	ttings	Window	w Help								
ign/E	ncrypt Decrypt/Veri	fy Imp	实 E port Exp	马 E ort Ce	rtify Lo	Q okup on Serve	Certificates	E Notepad	E Smartcards	Sroups					
Ente	r search term <alt+0< td=""><td>></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Al</td><td></td><td>~</td></alt+0<>	>											Al		~
[7	All Imported Co	ertificate	s												0
	N	ame					E-Mail		Status	alid From	alid Unt	Key ID			
	ONPOINT_HE	ALTH	DATA	_PR	supp	ort@onp	ointhealth	data.or	g certified	d 9/11/		B33B 9804 B	9		
	YourName				Ema	il@exam	ple.com		certif	. 5/2/	5/2/	C969 1F21			
						Testfile	y								

A Sign/Encrypt files dialogue will appear. The settings in this step are crucial. Doing this incorrectly will prevent Onpoint from decrypting the files and they will be rejected.

n Kleopatra	Sign/Encrypt I	Files - Kleopatra	×	-	D	×
File View Certificates	Sign / Encrypt Prove authenticity (sign)	Files				
Enter search term <alt+q> All Imported Certificates Name ONPOINT_HEALTH_ YourName</alt+q>	Encrypt for me: Encrypt for others: Encrypt with passwor	Convertence (Email@example.com> (certified, created: 5/2/2025) ConPOINT_HEALTH_DATA_PROD <support@onpointhealthdata.org> (certified, Open Please enter a name or email address d. Anyone you share the password with can read the data.</support@onpointhealthdata.org>		All		0
	Output Output files/folder: C:/Users/Adminis Encrypt / Sign each fil	itrator/Desktop 🛛	ß			
		Sign / Encrypt Can	cel			

The settings in this step are crucial. Doing this incorrectly will prevent Onpoint from decrypting the files and they will be rejected.

• Files sent to Onpoint must be ENCRYPTED with Onpoint's key and SIGNED with your key.

- Sign as: Select your key name from the drop down.
- Encrypt for Me: UNCHECK this box.
- Encrypt for others: Select Onpoint's key name (ONPOINT_HEALTH_DATA_PROD) from the drop down.
- Encrypt with Password: UNCHECK this box. Do no encrypt with a password.
- Output files/folder: Select a location to save the encrypted files.
- Encrypt / Sign each file separately: CHECK this box. We need the files encrypted separately.

An Encrypt-to-Self Warning will appear. Click Continue. You will not be able to decrypt the encrypted files because they now are encrypted with Onpoint's key. You will still be able to read your original files.

n Kleopatra	🙃 Sign/Encrypt Files - Kleopatra 🛛 👋		-	D	×
File View Certificates	Sign / Encrypt Files Prove authenticity (sign) Sign as: VourName <email@example.com> (certified, created: 5/2/2025) Sign as: Encrypt For For Encrypt For Fore Encrypt To-Self Warning - Kleopatra Finance Fore Fore Fore Fore Fore Fore Fore For</email@example.com>	All 39			> 0
	Output Output Output files/folder: C:/Users/Administrator/Desktop C:/Users/Administrator/Desk				

Sending Files to Onpoint Using PGP and SFTP

To send your encrypted files to Onpoint, you will need two applications: WinSCP and PuTTYgen.

WinSCP is an SFTP client that can be used to send the files to Onpoint and PuTTYgen – accessible within WinSCP – will generate an SSH key pair that will enable you to connect to Onpoint's SFTP server.

Generating an SSH Key Pair

Open WinSCP and In the Login window click the **Tools** menu and select **Run PuTTYgen**.



In the PuTTY Key Generator, you must select **RSA** as the key type and a minimum of **2048 bits** in the generated key.

Click Generate.

runn key General	tor		
ile Key Conversion	ns Help		
Key			
No key.			
Actions			
Actions Generate a public/private key	pair		Generate
Actions Generate a public/private key Load an existing private key file	pair		Generate Load
Actions Generate a public/private key Load an existing private key file Save the generated key	pair	Save public key	Generate Load Save private key
Actions Generate a public/private key Load an existing private key file Save the generated key Parameters	pair e	Save public key	Generate Load Save private key
Actions Generate a public/private key Load an existing private key file Save the generated key Parameters Type of key to generate:	pair e	Save public key	Generate Load Save private key
Actions Generate a public/private key Load an existing private key file Save the generated key Parameters Type of key to generate: O DS	pair e A O ECDSA	Save public key	Generate Load Save private key O SSH-1 (RSA)

While the generator is running, move your mouse randomly. This creates randomness for your key.

PI	uTTY Key	Generator				
File	Key Co	nversions	Help			
Key						
Put sst +N TZ oJ +h	blic key for past 14sa AAAAB3N efkxtIAX67ioM EaSvRMSuZh 1asm1+2M91o1 Pdf6cc/LdfkGI	ing into OpenSS izaC1yc2EAAAA bg5nTVD9ihLx2 GIFS7ogtJppGw E7FQyPIOrZrAm .d0ijWq5Rt2k0V	iH authorized_keys file: IDAQABAAABAQCmAaT 2WyD2bwVusHNBD0c6 rySW/FT7843IEqUMxDa r0hocBKXG6iM0SBvhXI WspOPPRTrkXjsIIF2s425	oljWXipp1yCfar8Tu1cjWEQdl r3hPVNn5zS3rdYgWbT25nvv 1 ftufVF9BlWYTJWyIDzz4kyN EdDKyRZdK 9rPkwC6vRdzi/ECPfEy1tsVbyr	JqNy8ckqYF JFY3nF4w1nlG6ddBoM MNXcEBCL0GCXinRwM mWI7U5JX rsa-key-	
Key	fingerprint:	sshirsa 2048	SHA256:aJfOQoVBusy	QkD86yHhSO8Fr/TTXjX3TP9	Mw50om7y0	
Key	comment:	rsa-key-2025	50502			
Key	passphrase:					
Cor	nfim passphras	e: b3				
Acti	ons					
Acti Ger	ons nerate a public.	'private key pair			Generate	
Acti Ger Loa	ons nerate a public. Id an existing p	/private key pair ivate key file	4.		Generate Load	
Acti Ger Loa Sav	ons nerate a public; id an existing p ve the generate	'private key pair rivate key file d key		Save public key	Generate Load Save private key	
Acti Ger Loa Sav Par	ons nerate a public, id an existing p re the generate ameters	lprivate key pair rivate key file d key		Save public key	Generate Load Save private key	
Acti Ger Loa Sav Par Typ	ons herate a public/ ad an existing p ve the generate ameters be of key to ger RSA	/private key pair rivate key file d key erate: DSA	○ ECDSA	Save public key	Generate Load Save private key	

You can create a passphrase (shown in the screenshot above), which is not required but is more secure. Like the passphrase for your PGP key pair, this passphrase cannot be recovered. If it is lost, a new SSH key must be generated.

Save the public key and send it to Onpoint. Save the private key and keep it for yourself. Never share with anyone, including Onpoint.

Upon receipt of your SSH key, Onpoint will use it to create your SFTP account.

Logging into the SFTP Server

🔁 Documents – WinSCP				- 0 ×
Left Mark Files Command	ls Tabs Options Right Help			
🕀 🔚 📷 Synchronize 🗖	🐙 🗷 🔷 🖗 Queue - Tra	nsfer Settings Default 🔹	18 -	
📋 Documents – Documen	ts 📡 New Tab 🔹			
🗟 My docum 🕶 📁 🕶 💌 🕶	월 Login		- 0 - x 15	🕽 🗎 Find Files 🚼 🛅
💚 Copy + 🛛 Edit + 🗙 😖 C:\Users\Administrator\Doc	New Site TestUSer1©transfer.onpointhealthdata.org	Session File protocol:	15	New 🛛 💽 🖃 💟
Name Size		Host name: transfer.onpointhealthdata.org	Port number:	Changed 4/3/2025 7:59:4
		VourSFTPUsername Save	Advanced	
	Tools Manage	2 Login ▼ 0	Clos	ion ngs igs Rule iferences
) B of 0 B in 0 of 0		4 hidden 0 B of 0 B in 0 of 0		4 hidde

When you open the WinSCP application, a login screen appears. Enter the following information into the appropriate fields:

- File protocol: SFTP
- Host Name: transfer.onpointhealthdata.org
- Port number: 22
- Username: The username you were given by Onpoint when your account was created.
- Password: Leave blank instead click **Advanced** and select **Advanced** from the drop-down men.

In Advanced Site Settings, go to the Authentication tab. In the Private key file field, click the three dots (...) in the lower right corner.

	Allow GSSAPI credential dele	n egation		
	GSSAPI			
				(44)
Note	Certificate to use with the private	cey:		
- Bugs	Display Public Key	Tools	•	h
- Key exchange Authentication				C.R
SSH	Private key file:			
Tunnel	Allow agent forwarding			
Connection	Authentication parameters			
Shell	Respond with a password to	the first prom	pt	
- SFTP	Attempt 'keyboard-interactive'	authentication	ı	
- Recycle bin	Attempt authentication using f	ageant		
- Directories	Authentication options			
Environment	Bypass authentication entirely			

In the selection box that pops up, select your private SSH key from wherever you have saved it. Click OK.

🐁 Select private key	file					×
← → ∽ ↑ 🛅	> Desktop > PGP&SFTP > 2	Keep for yourself - pr	ivate		~ C	Search 2 Keep for P
Organize • New f	older					≣ • □ 0
A Home	Name	Date modified	Туре	Size		
🖪 Gallery	PRIVATE-SSH_demo.ppk	1/21/2025 9:35	PPK File	2 KB		
	PrivateSSHKey.ppk	5/2/2025 6:53	PPK File	2 KB		
 Desktop Documents Downloads Pictures Music Videos 	Type: PPK File Size: 1.57 KB Date modified: 5/	2/2025 6:53 PM				
> 📮 This PC > 🙀 Network						

If you set a passphrase for your SSH key, you will be prompted to enter it. You are now logged into Onpoint's SFTP Transfer Server. You will see a PROD and TEST Directory.

😼 / – TestUSer1	@transfer.or	npointhealthdat	a.org – WinSCP				-	o x
Local Mark File	es Comman	ds Tabs Option	s Remote Help					
🕀 🈂 📚 Synch	hronize 🗾	🦻 😰 🚺 💣	Queue - Transfer S	ettings Default	• 🔊 •			
TestUSer1@t	transfer.onpo	ointhealthdata.c	org × 礕 New Tab 🔸					
My docum •	··		a G 💺 🗖 🗸	 / < • • •	++++ B	D 🏫 🖸	Rind File	es 🔁 📖
Upload -	🕈 Edit - 🗙	🖌 🕞 Propertie	s * * * • •	Download •	🛛 Edit • 🗙 🛃	Properties	5 • »	+ - 1
C:\Users\Admini	strator\Docu	iments\		/				
Name	Size	Type Parent direc	Changed 4/3/2025 7:59:4	Name	Size Chan 11/24] 11/24	ged //2021 4:48 //2021 4:48	Rights rwxrr rwxrr	Owner -
0 B of 0 B in 0 of	f 0		4 hidd	en 0 B of 0 B in 1 of 2				

Sending Files to Onpoint

To send a test file, enter the TEST directory and drag and drop a file from your computer into it.

::\Users\Admini	strator\Docu	ments	/TEST/					
Name	Size	Typ Upload		?	×	əd	Rights	Owner
2		Par Upload file 'TestFile.txt.gpg' to remote TEST/** Transfer settings Transfer type: Binary Transfer in background (add to transfer q Transfer settings	e directory:	Hel	p)25 6:32:)25 6:32:)25 6:37:)25 9:47:	rwxrr rwxrr rwxrr rwxrr	

Click **OK** in the Upload pop up.

Once you have uploaded the test file, you may see the following error message:

Error				? ×
8	Upload of file occurred while timestamp. If the problem per timestamp. Altern option.	'TestFile.txt.gpg le setting the pe rsists, turn off settin natively you can turr	g' was successfu ermissions and/o g permissions or pres	l, but error or erving on errors'
	-	at summer the summer		
	Error code: 8 Error message fro	om server (US-ASCII)	ation. : SETSTAT unsupport	ed 🗸
A	Error code: 8 Error message fro	om server (US-ASCII) y Skip	ation. : SETSTAT unsupport Skip all	ed Help

This error occurs because WinSCP tries to change the properties of the submitted file after it has been sent to Onpoint. You have two options for dealing with this error. First, you can ignore it by selecting **Skip All**. At this point, Onpoint has already received the file, and this error does not affect Onpoint's ability to receive or process the submission.

To no longer see this error, you can go to **Options > Preferences** in WinSCP. Select the **Transfer** tab and click **Edit** with the Default transfer settings selected. In the **Transfer Settings** pop up, uncheck the **Preserve timestamp** box.

Search	Transfer settings presets		
Environment	Preset description	A	uto
Interface	Default		
Window Window Commander Explorer Languages Panels File colors Remote Local Editors Internal editor Transfer Drag & Drop Background Endurance Network Security Logging Integration Applications Commands	Text Binary New and updated files only Exclude directories Transfer type: Binary Add Edit	Transfer settings Transfer mode Text (plain text, html, scripts,) Binary (archives, doc,) Automatic Transfer following files in text mode: *.*html; *.htm; *.txt; *.php; *.php3; *.cgi; *. Upload options Set permissions: nw-rr (+x) Ignore permission errors Clear 'Archive' attribute Remove BOM and EOF marks E Encrypt new files	 ? × Filename modification No change Upper case Lower case Lower case 8.3 ☑ Replace "\:*?' Common options Preserve timestamp Including directories ② Calculate total size Speed (KB/s): Unlimited Download options Preserve read-only
Updates	Announce when transfer se	Other File <u>m</u> ask:	∽ Edit
idden 0 B of 2	.19 KB in 0 of 5	New and updated files only Exclude empty directories	mask hints