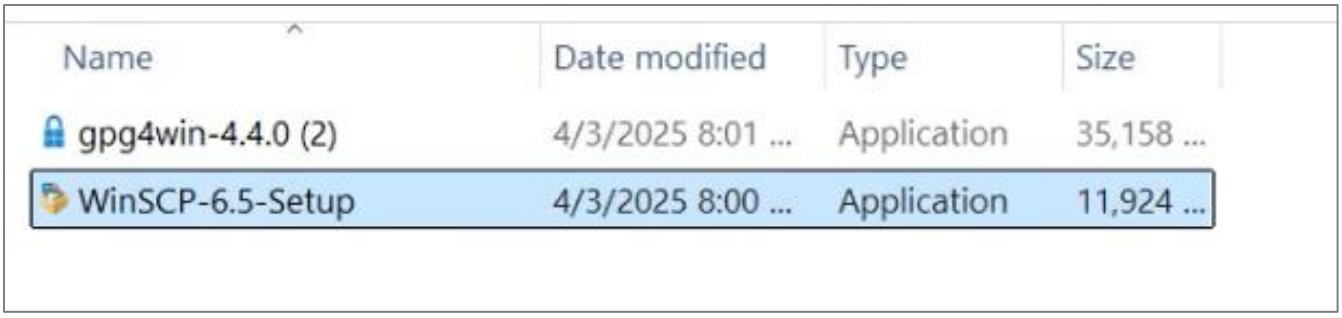
ONPOINT Health Data | Support Documentation

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.

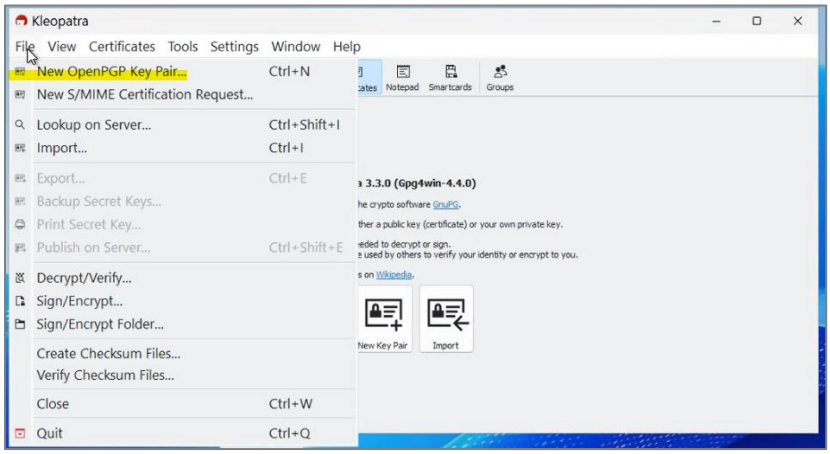
Getting Started

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.



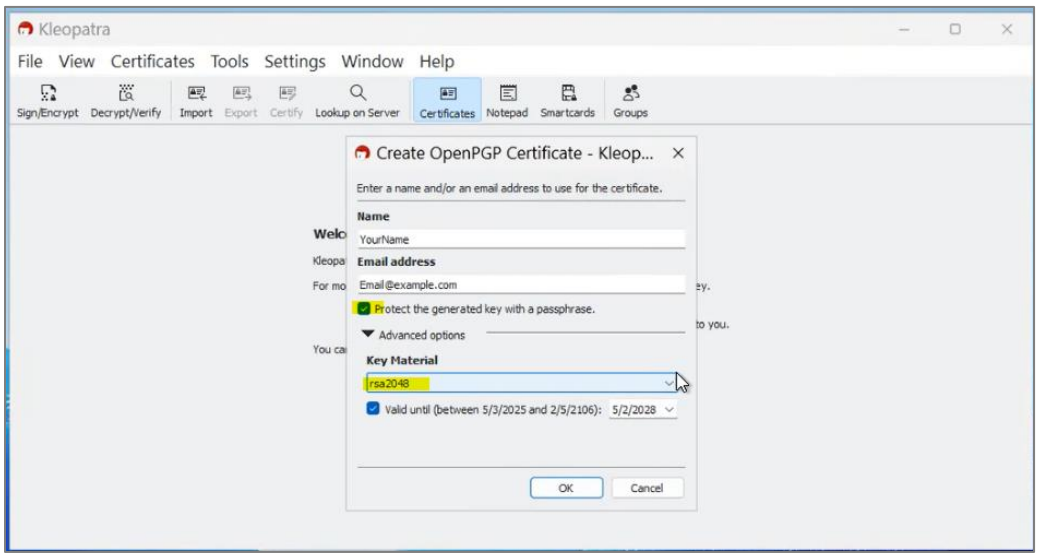
Creating a PGP Pair

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.

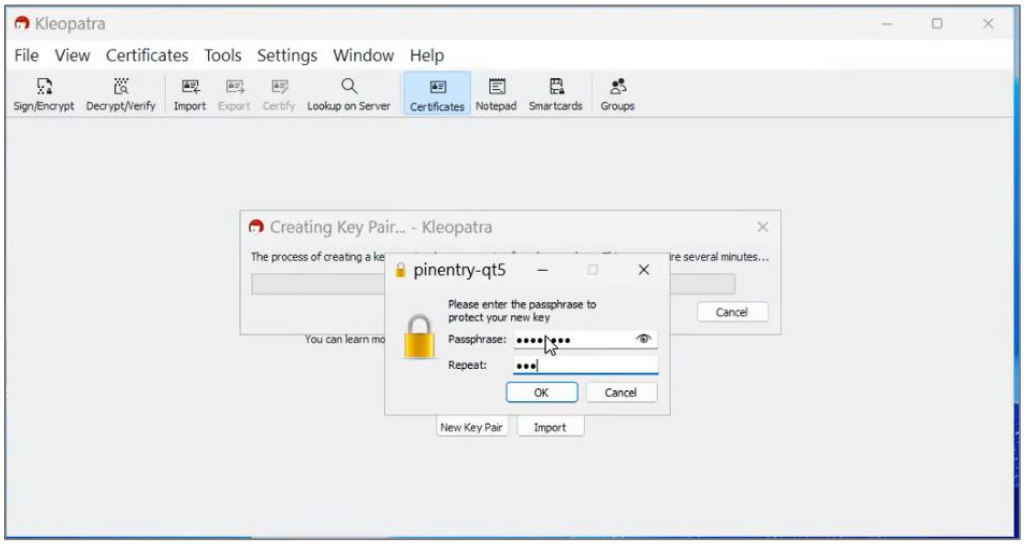
You may choose to protect the key with a passphrase. This is not required, but it is recommended for security. If you set a passphrase, you must store it securely for later use. You will need to enter the passphrase whenever you encrypt or decrypt files using the key. The passphrase cannot be recovered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



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.

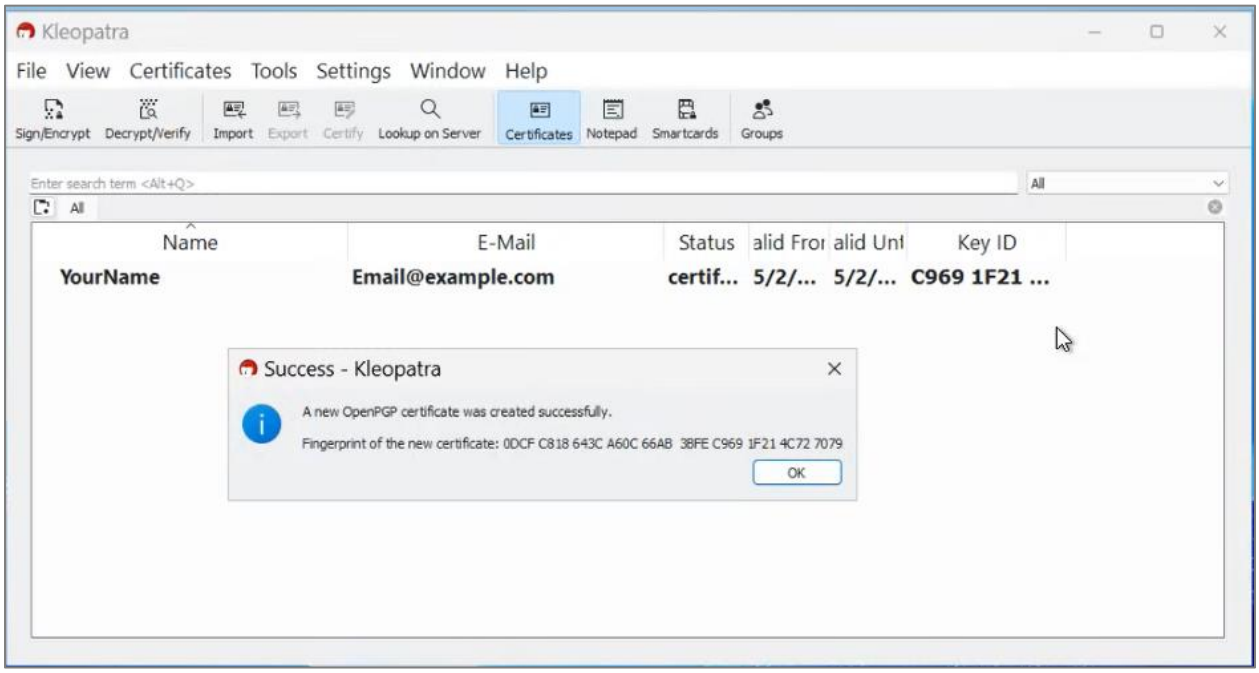
You have the option to set an expiration date for your key pair. When the key expires it can no longer be used for encryption and a new key must be generated and provided to Onpoint. Expiration is not required but is recommended for security. You can adjust the length of key validity to your preference 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.

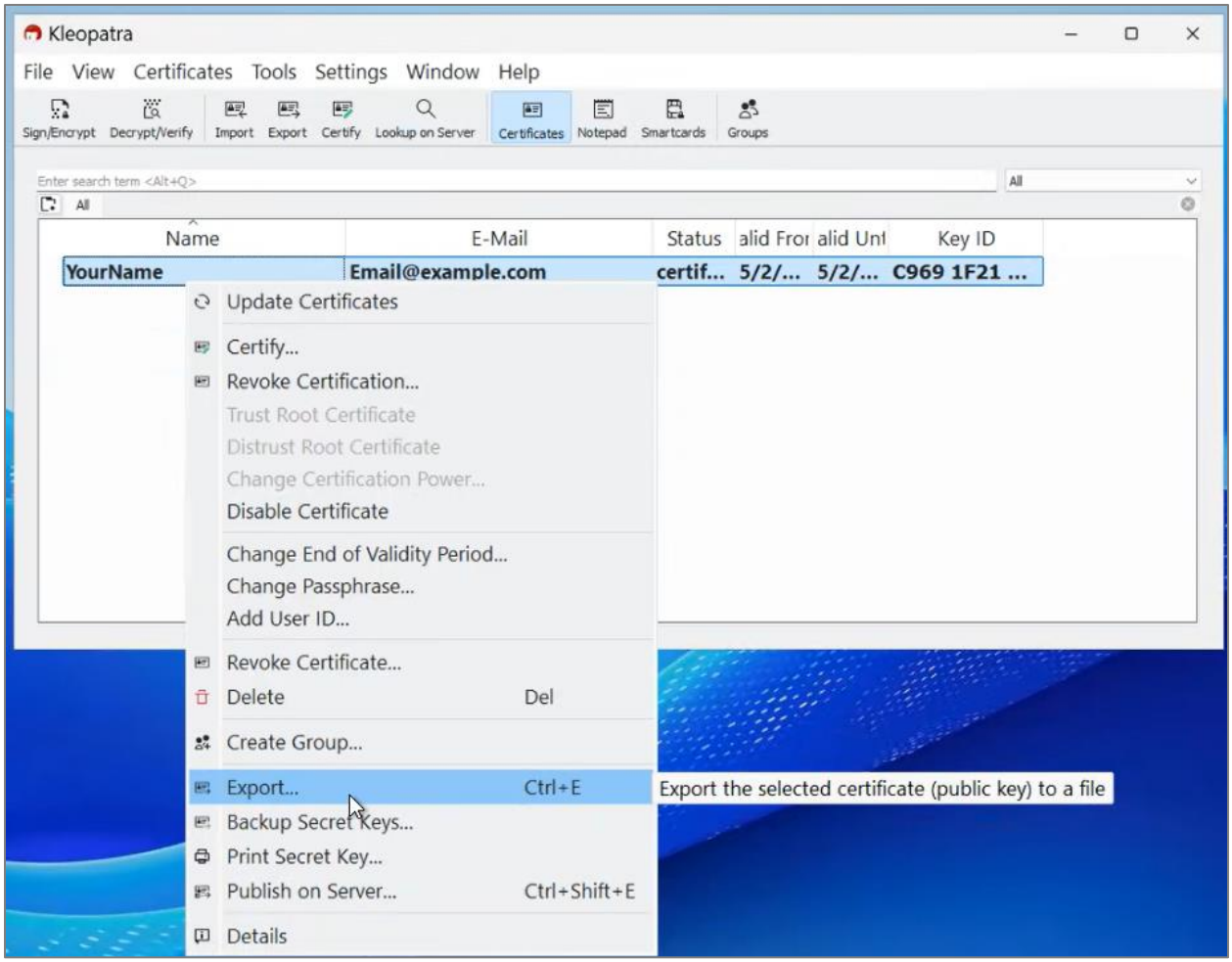


After entering a passphrase, a pop up will appear showing that a keypair has been created successfully.

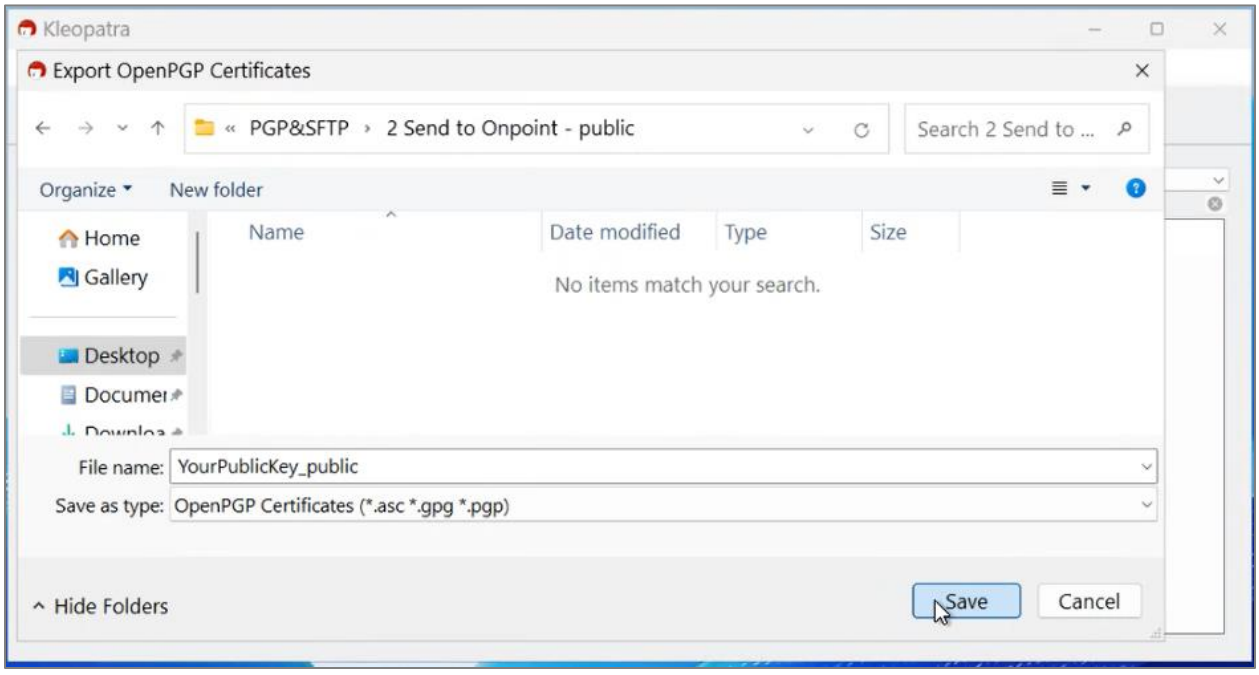
In the Kleopatra Certificates pane, you will now see your new keypair listed in bold. The bold text indicates that you hold both the private and public half of this key pair.



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.



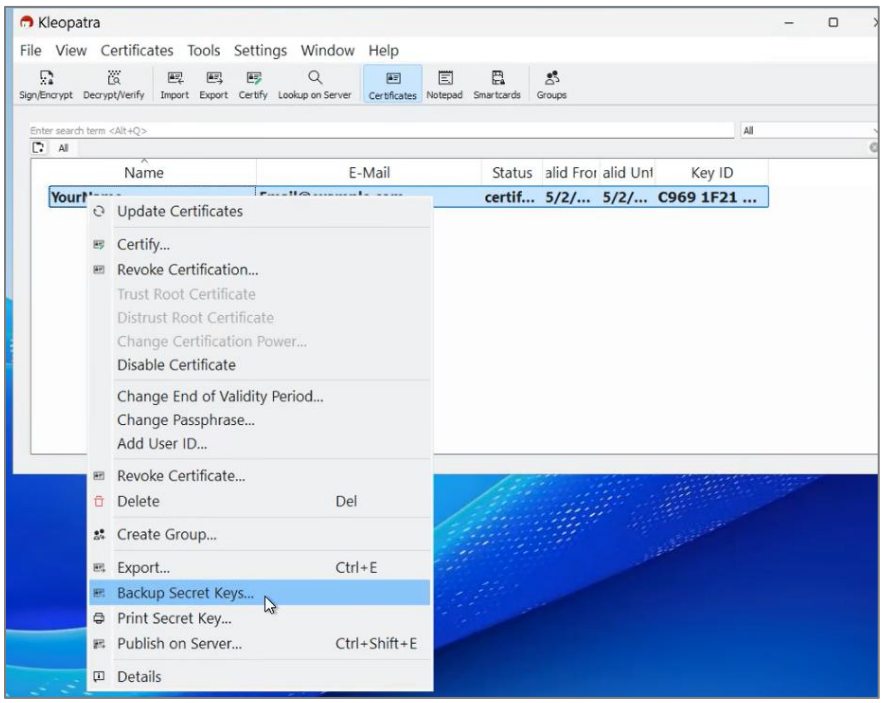
Save the key. We strongly recommend including the word “public” in the key name so that you can differentiate it from the private key.



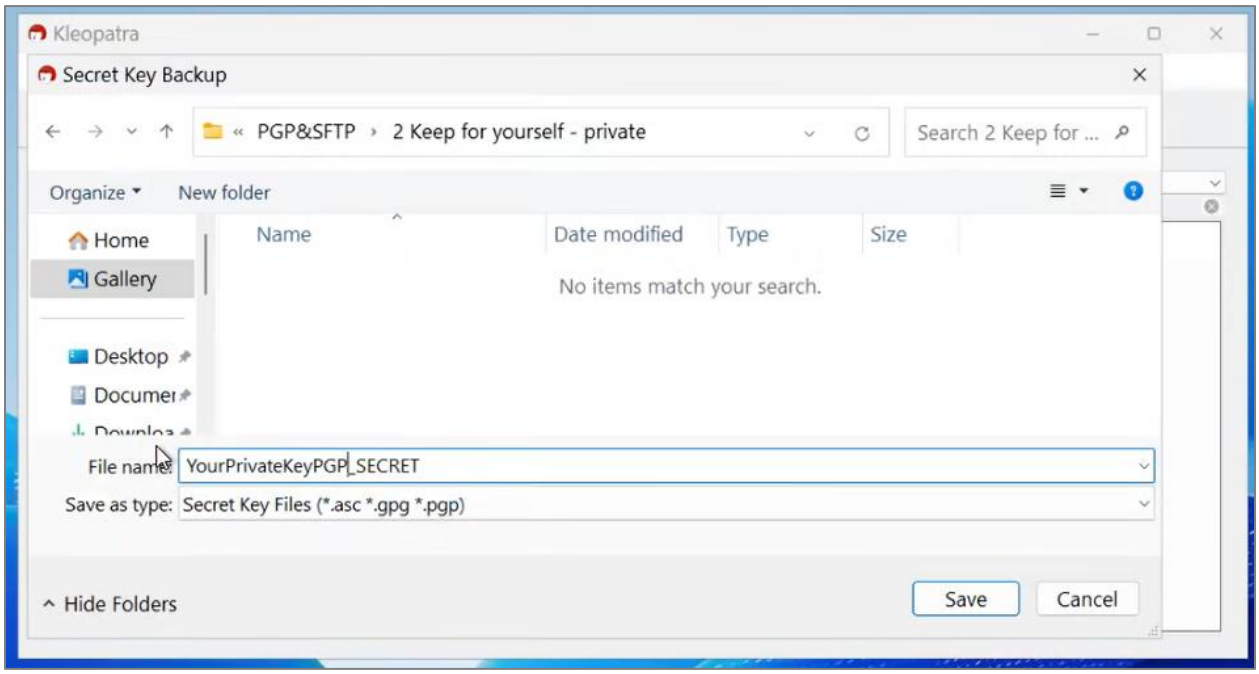
Once the public key has been exported and saved, send it to Onpoint along with your SFTP account registration.

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



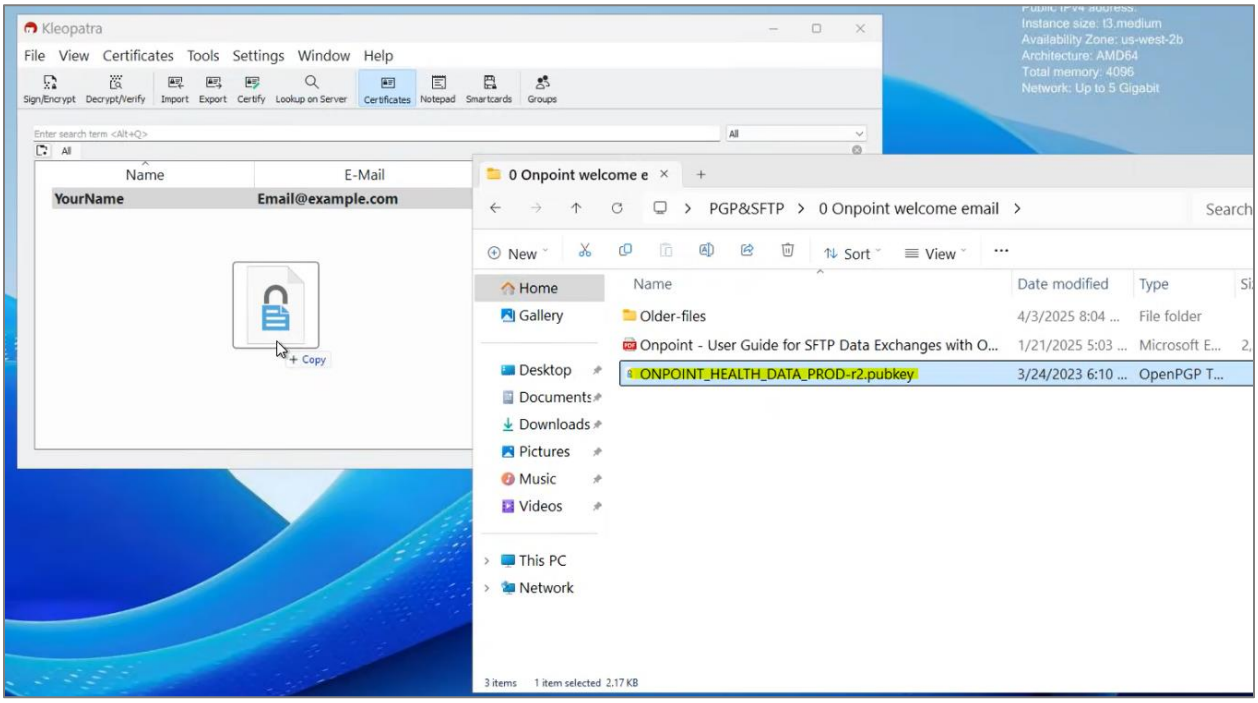
Save the private key. We strongly recommend including the word “private” in the key name. A private PGP key should be treated as if it were a password. It should never be shared with anyone (including Onpoint). **Do not send the private half of your PGP key pair to Onpoint.**



Importing Onpoint's Public Key into Kleopatra

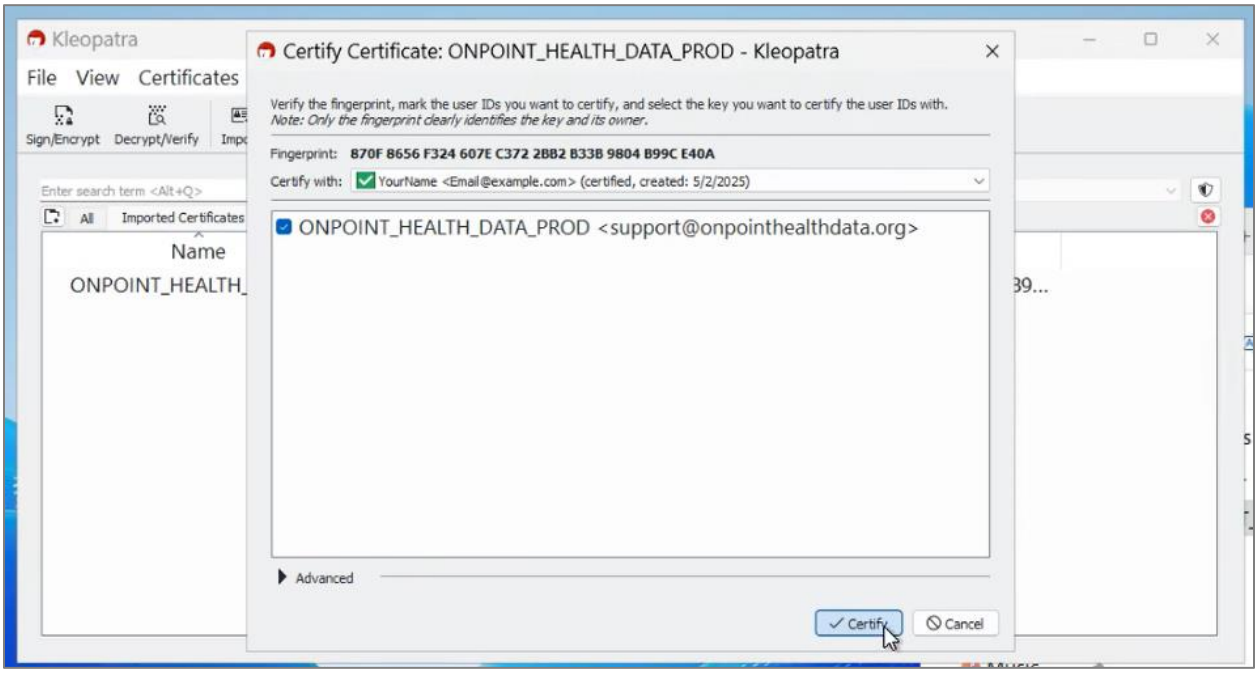
When you send files to Onpoint you will encrypt them using Onpoint's public key. To do this, you must import the public key you received in the Onpoint welcome email into Kleopatra.

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

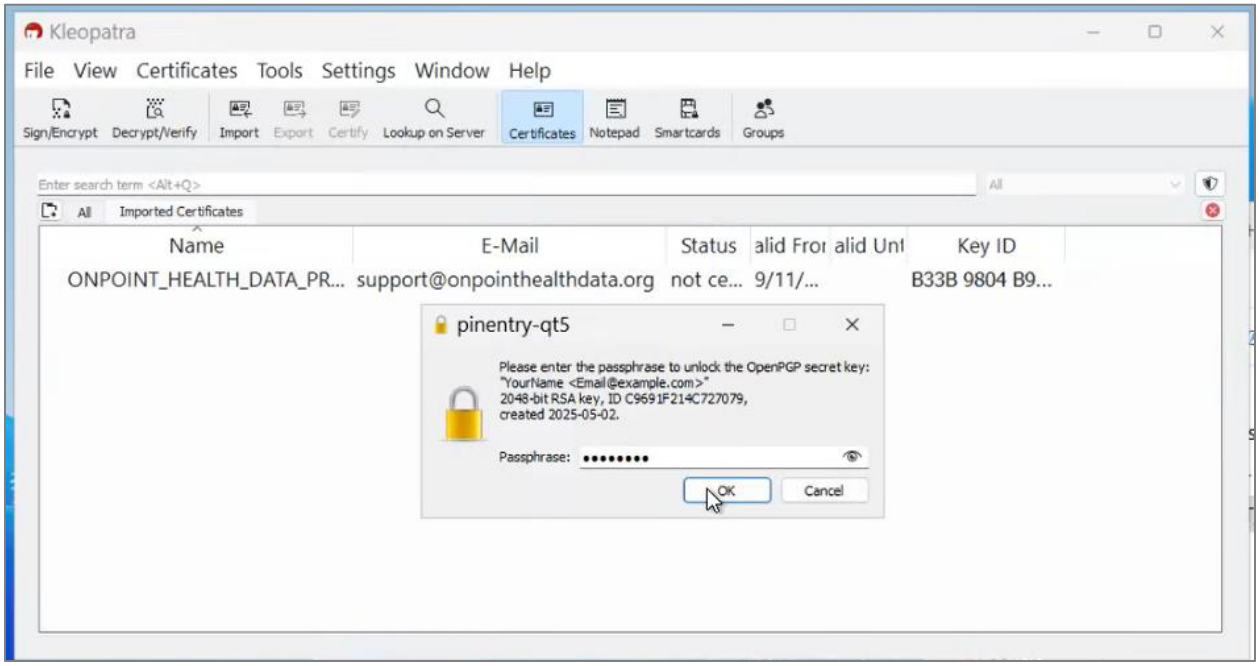


You will be asked to certify the key you are importing. Certification means that you trust that the key belongs to the person who sent it to you. It is important to take this step after creating your own key because you will use your key to perform the certification.

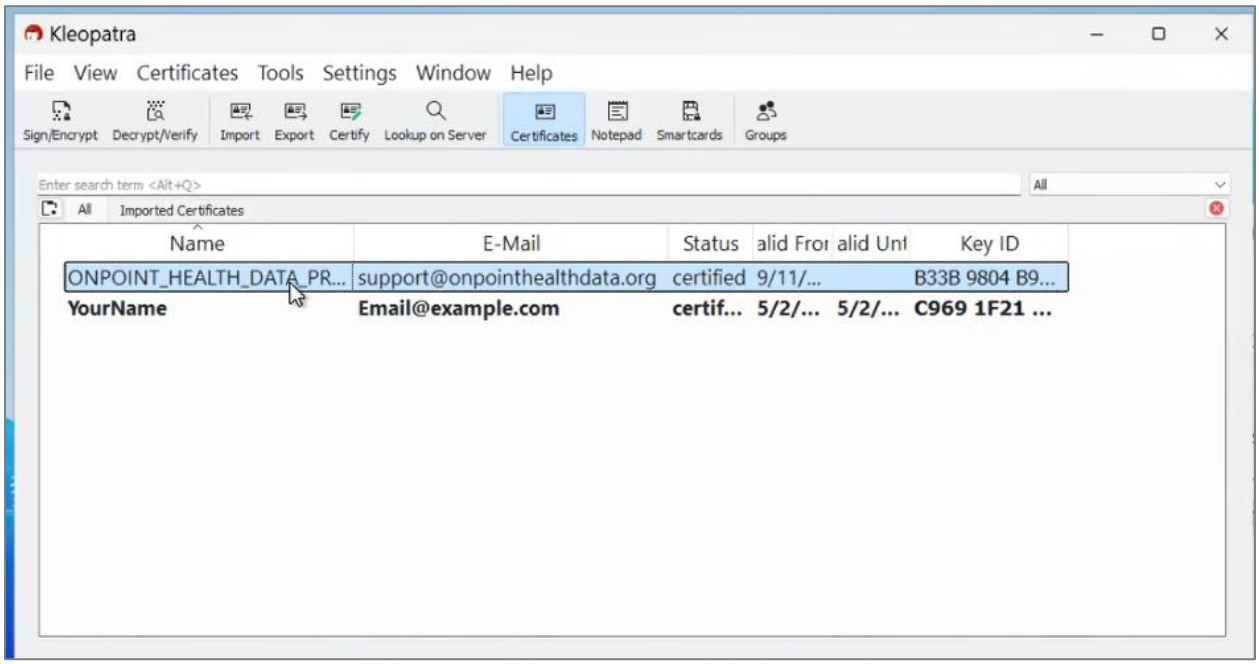
Select your key name from the **Certify with** drop down. Click **Certify**.



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



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

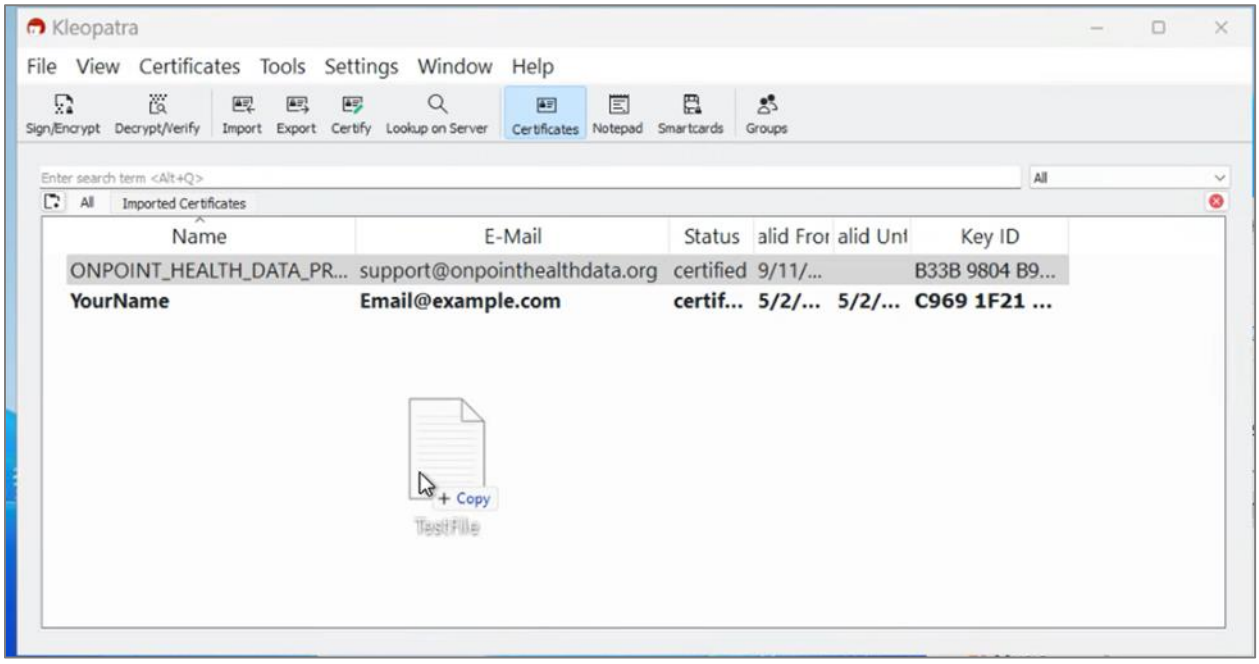


Notice that it is not in bold text. This is because you have only the public half of the key pair. This means you would not be able to use this key to decrypt.

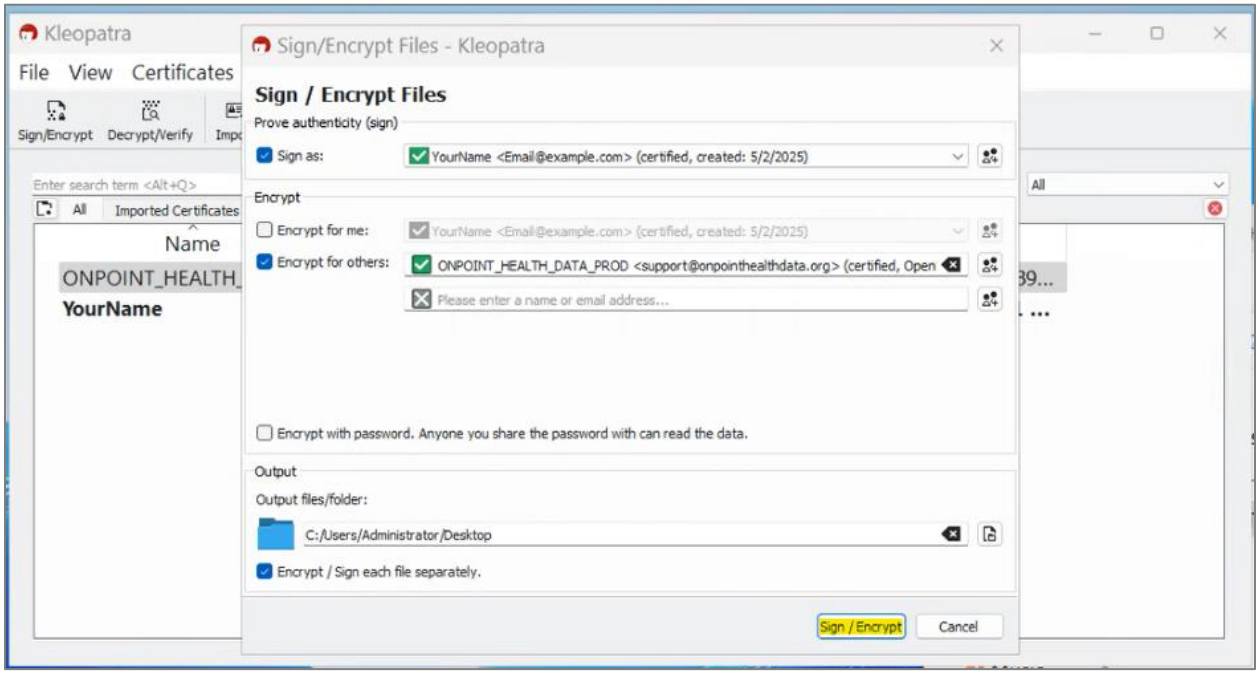
You now have your key pair set up and Onpoint's public key imported. You are ready to encrypt files.

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.



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.

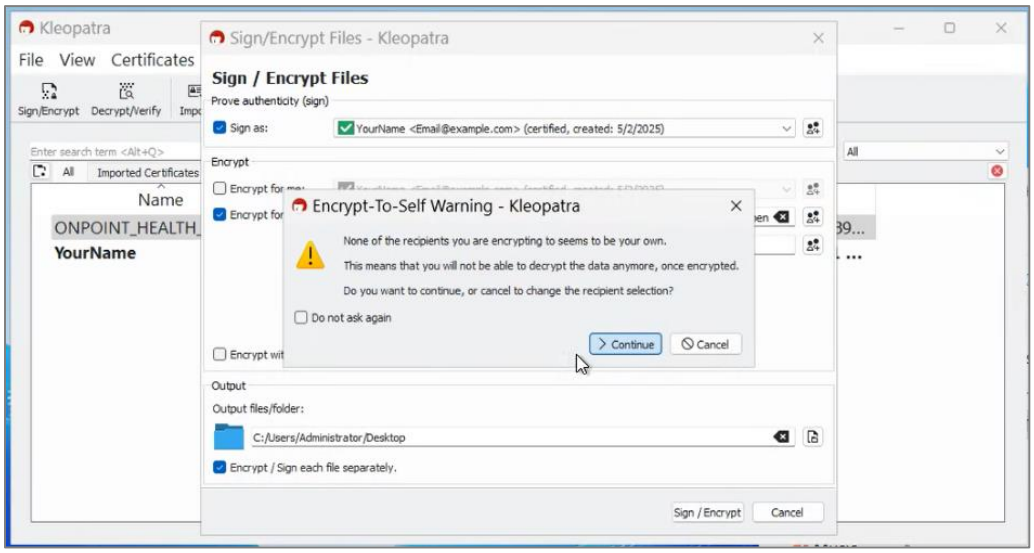


The settings in this step are crucial. Doing this incorrectly will prevent Onpoint from decrypting the files and they will be rejected.

- 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.



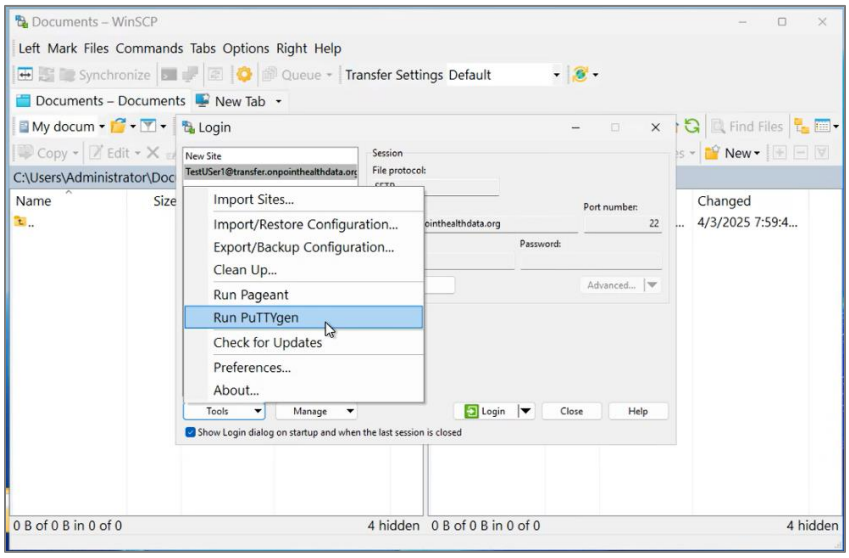
Sending Files to Onpoint Using PGP and SFTP

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.

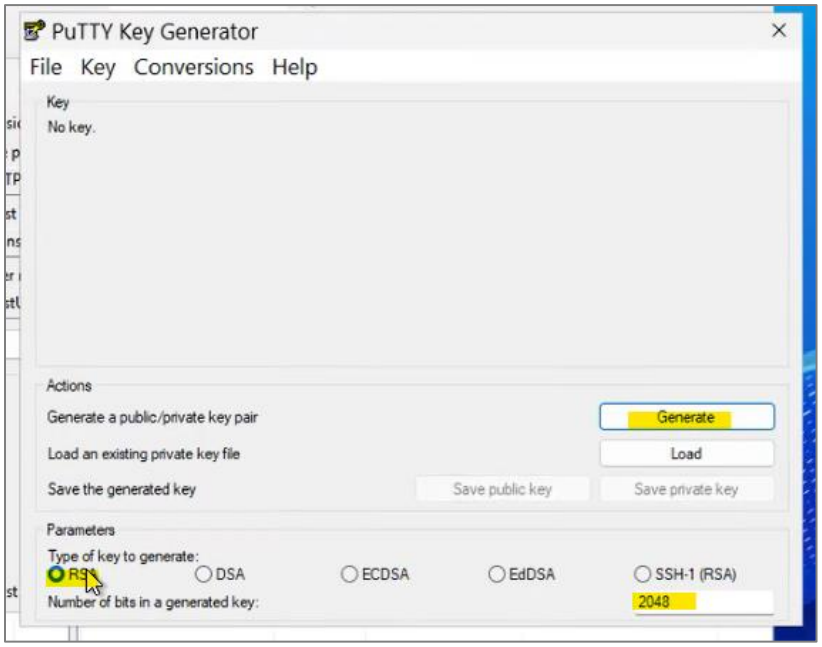
Generating an SSH Key Pair

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

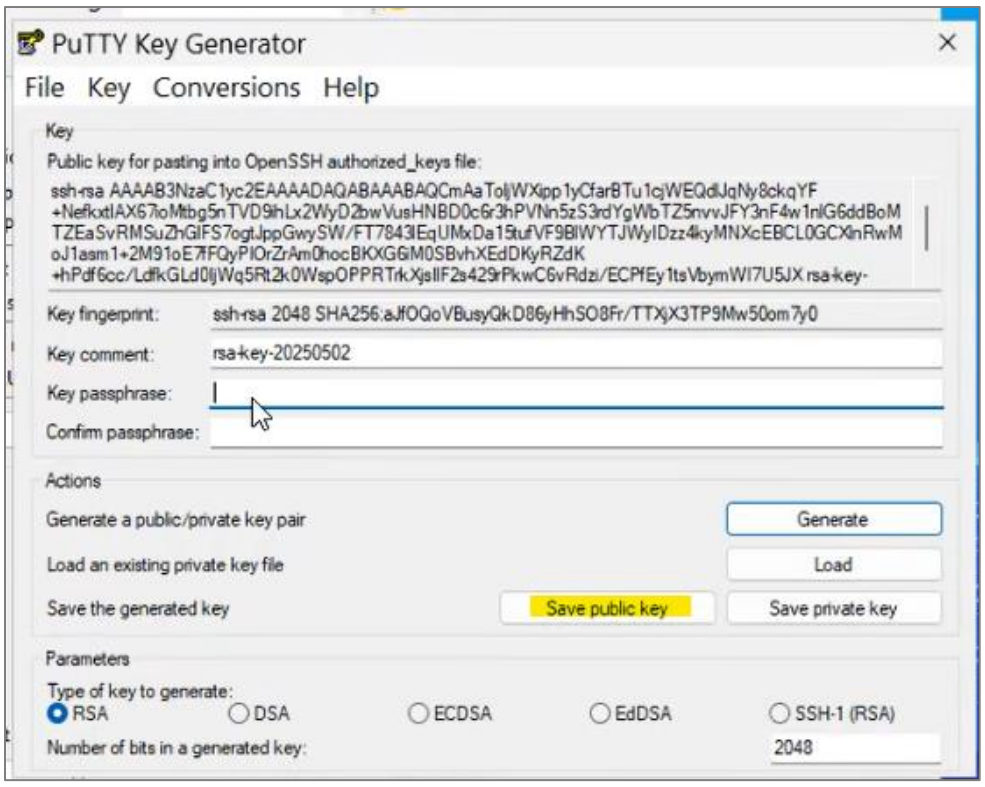


In the PuTTY Key Generator, you must select **RSA** as the key type and a minimum of **2048 bits** in the generated key.

Click **Generate.**



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

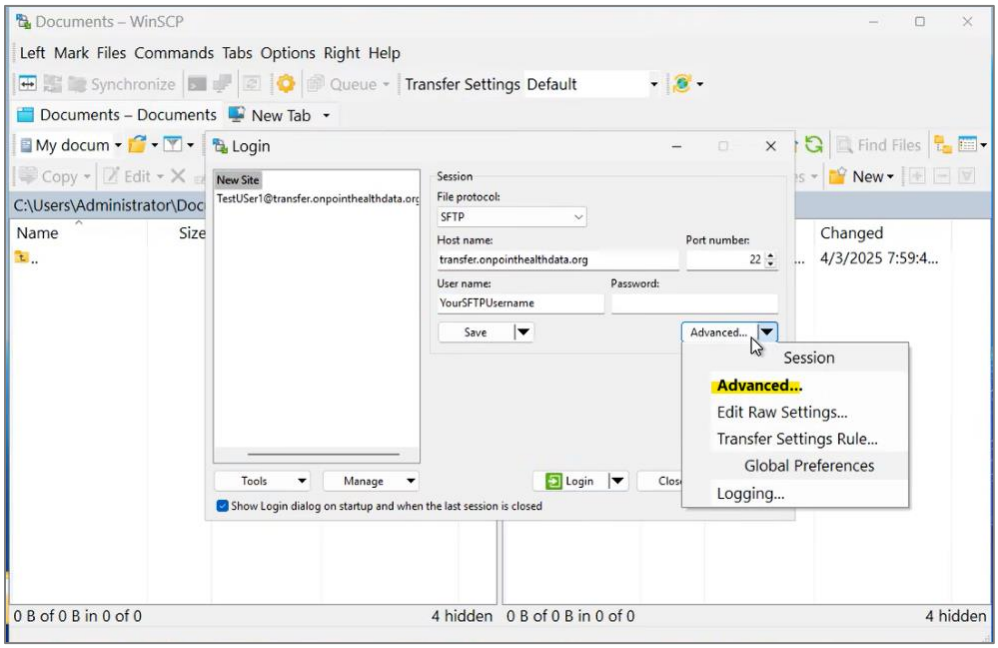


You can create a passphrase (shown in the screenshot above), which is not required but is more secure. Like the passphrase for your PGP key pair, this passphrase cannot be recovered. If it is lost, a new SSH key must be generated.

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.

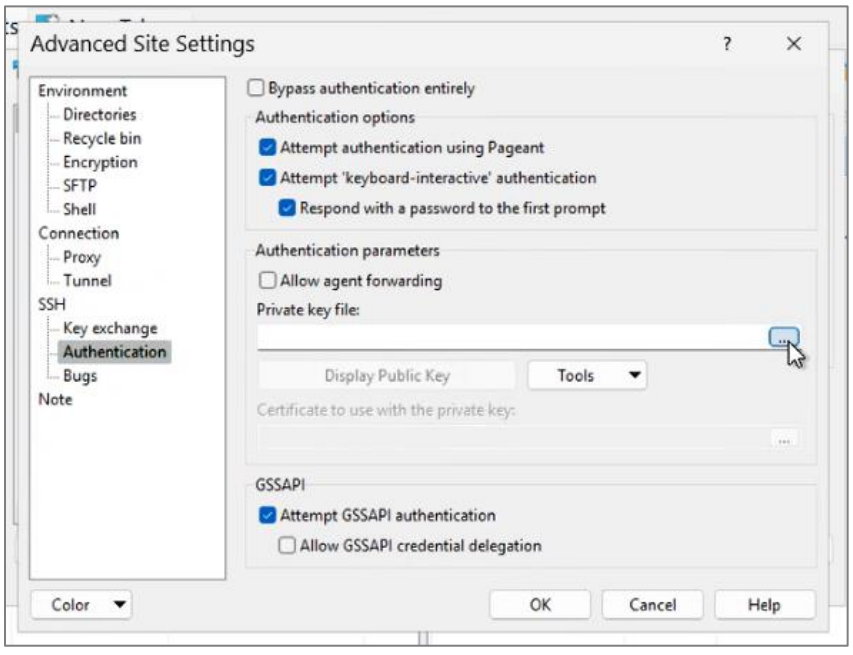
Logging into the SFTP Server



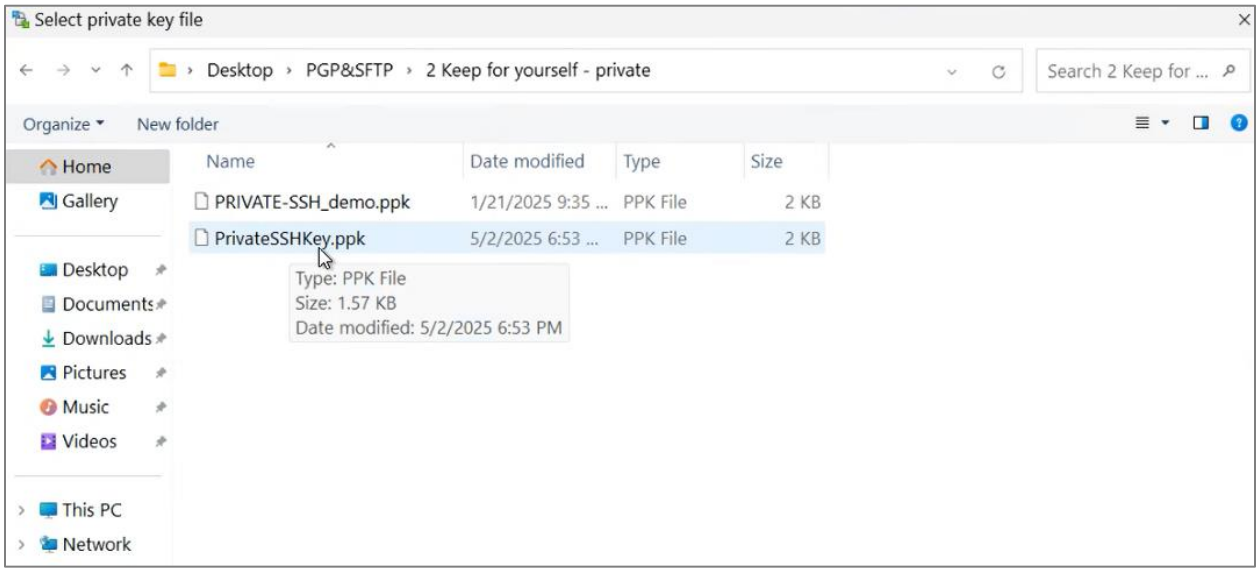
When you open the WinSCP application, a login screen appears. Enter the following information into the appropriate fields:

- 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.

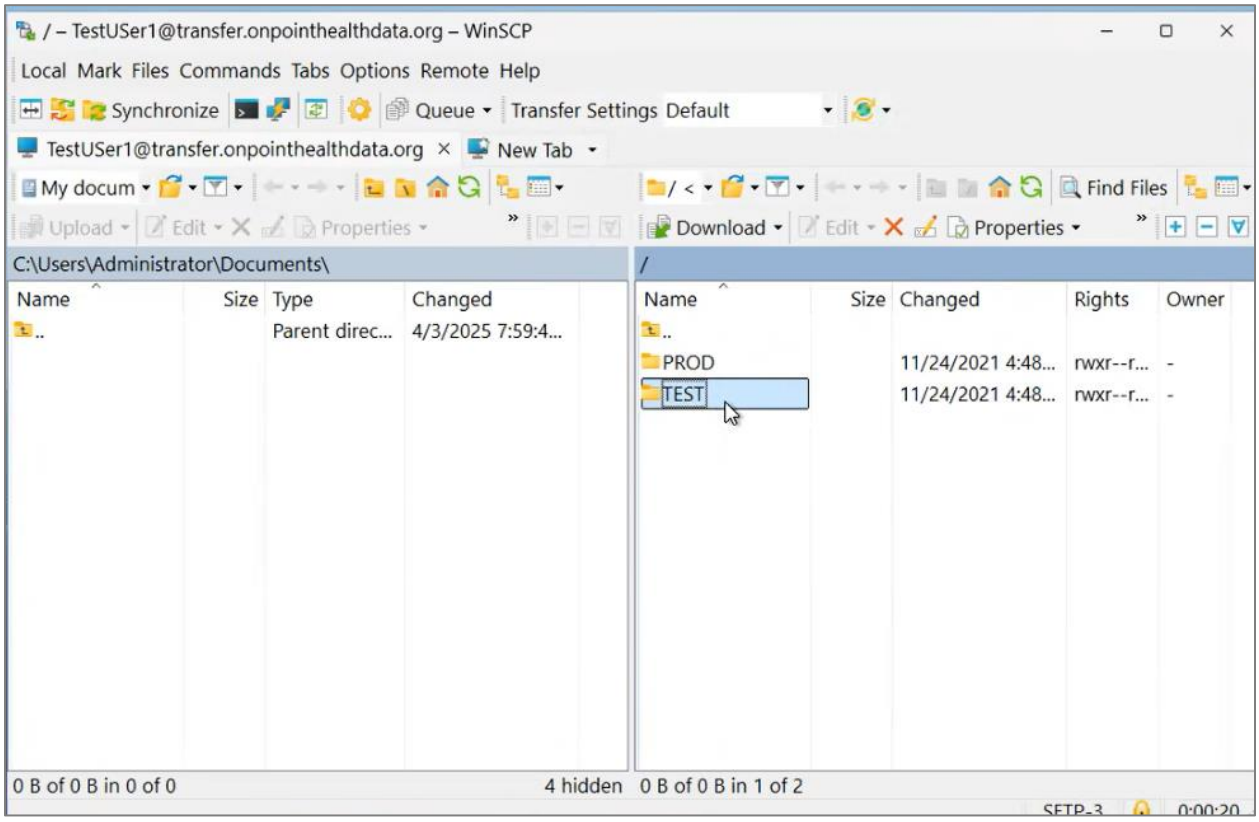
In Advanced Site Settings, go to the Authentication tab. In the Private key file field, click the three dots **(…)** in the lower right corner.



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

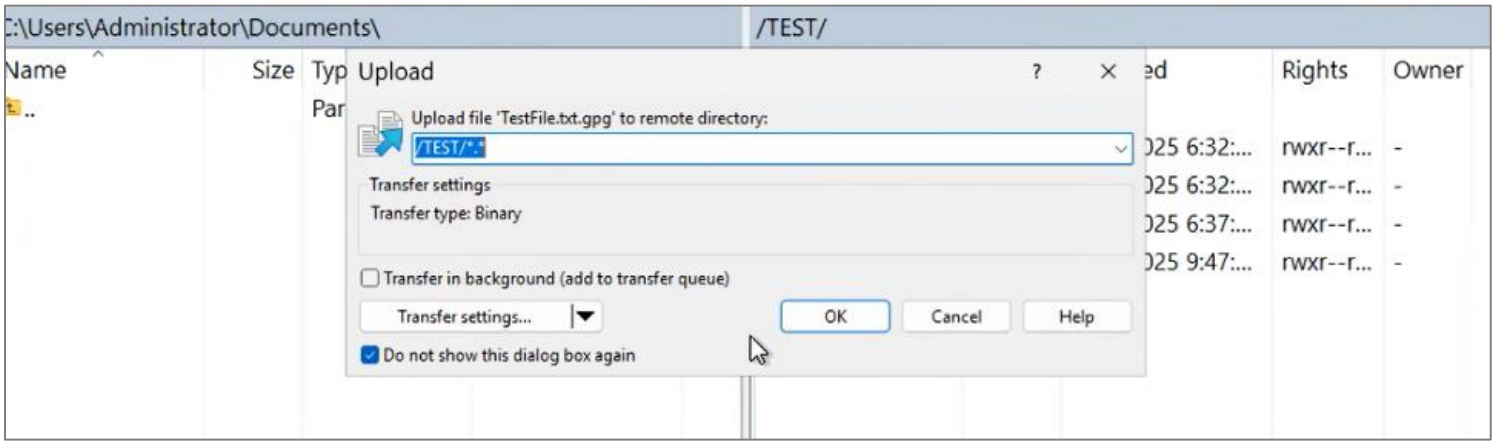


If you set a passphrase for your SSH key, you will be prompted to enter it. You are now logged into Onpoint's SFTP Transfer Server. You will see a PROD and TEST Directory.



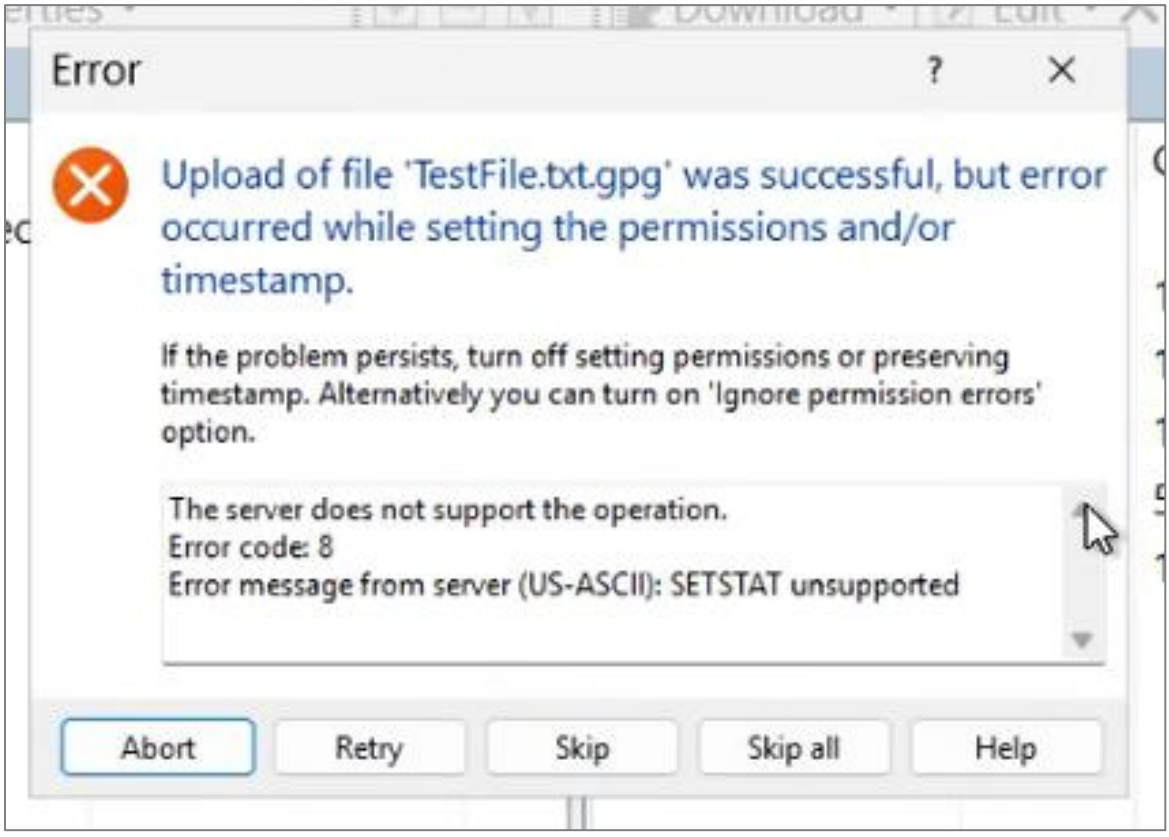
Sending Files to Onpoint

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



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

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



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.