SUNY RF
The Research Foundation for
The State University of New York

Cloud Migration & Oracle Upgrade Project

Training Guide

SFTP

Introduction

With public key authentication, the authenticating entity has a public key and a private key. Each key is a large number with special mathematical properties. The private key is kept on the computer you log in from, while the public key is stored on the computer you want to log into. When you log into a computer, the SSH server uses the public key to encrypt your connection in a way that can only be decrypted by your private key — this means that even the most resourceful attacker can't snoop on, or interfere with, your session. As an extra security measure, most SSH programs store the private key in a passphrase-protected format, so that if your computer is stolen or broken into, you should have enough time to disable your old public key before they break the passphrase and start using your key.

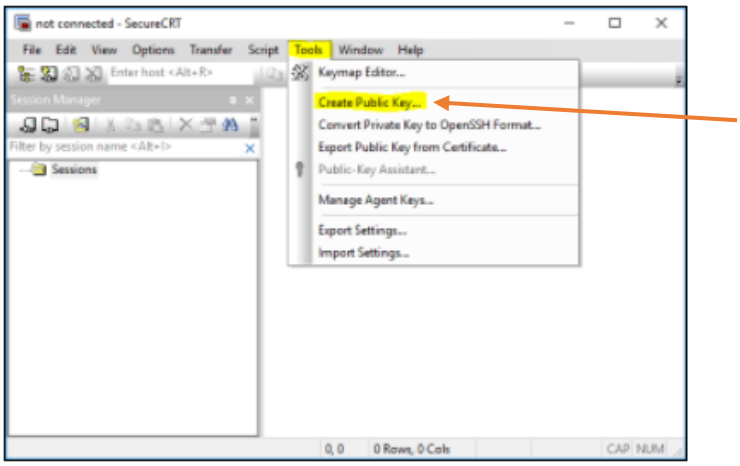
Overall Process

1) Generate key pair
2) Send public key to RF ITS
3) Configure SecureCRT/SecureFX to use new keys (for Windows users)

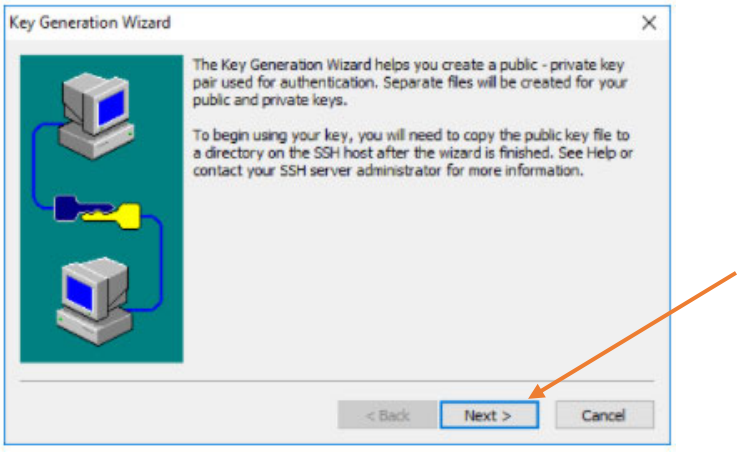
Generate Key Pair

SecureCRT (Windows)

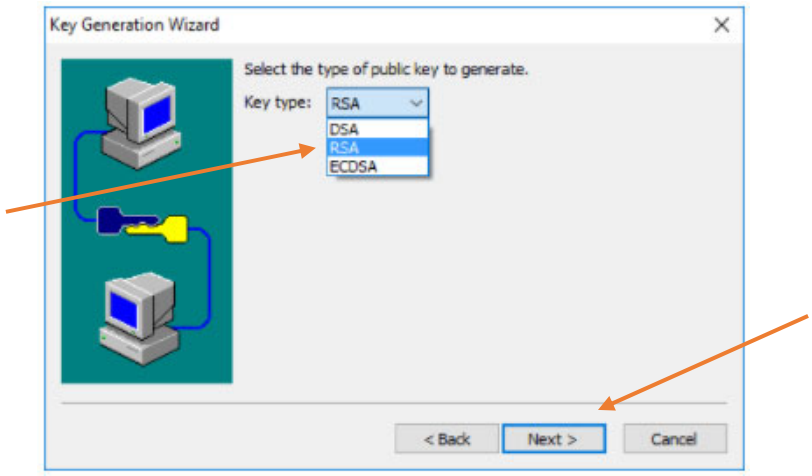
1 **Start SecureCRT. Under the Tools menu, select Create Public Key.**



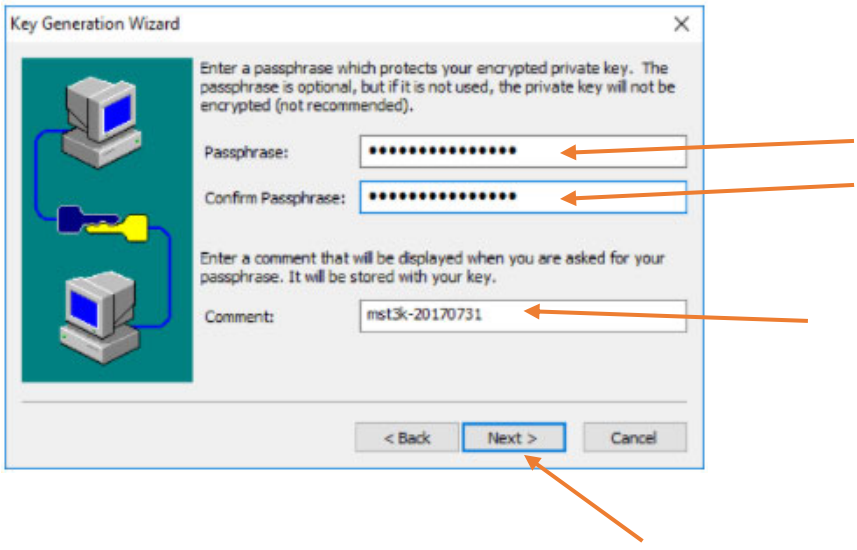
2 **Click Next.**



3 In the **Key type** dropdown, select **RSA** and click **Next**.

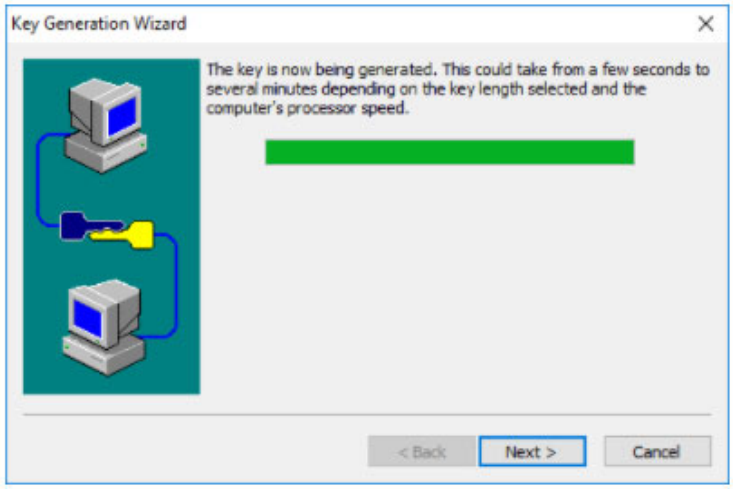


4 Enter a strong passphrase in the **Passphrase** box and then enter it again in the **Confirm Passphrase** box. Be sure to securely save this passphase as you will need to enter it each time you use your keys. Enter a comment to help you identify your key. Click **Next**.

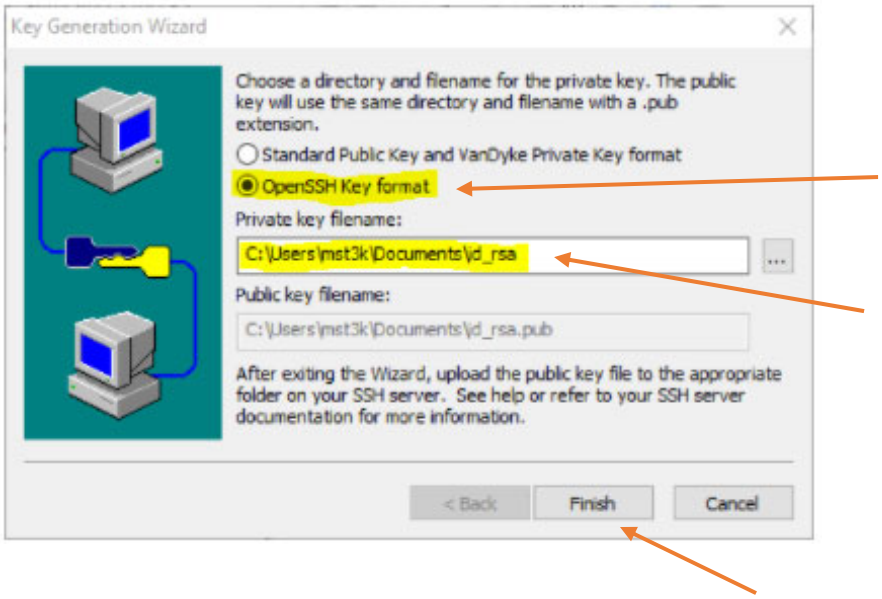


5 Enter the key length. If you are using SecureCRT 7.3 or later, enter **4096**. If you are using an older version, enter **2048**. Click **Next**.

6 Your key will now be generated. When it finishes, click **Next**.



7 You will now be asked which format you would like to save your key pair as and what to name it. **IMPORTANT:** Choose OpenSSH Key format and name your private key **id_rsa**. Note where your keys are being saved (you will need this for the next step). Click **Finish**.



8 Send your public key (id_rsa.**pub** file) to RF ITS Managed Systems: managedsystems@rfsuny.org.

macOS or Linux

1. On your computer, open a terminal (located in the Applications/Utilities directory). In your home directory, run the following command:

```
[mst3k@servo:~]$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
```

2. You will then be asked some questions. Note that the path to your home directory may differ from the example. You want to enter a passphrase to protect your key pair. Be sure to securely save this passphrase as you will need it each time you use your key.

```
Enter file in which to save the key (/Users/mst3k/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

3 The command will then output some info and your keys:

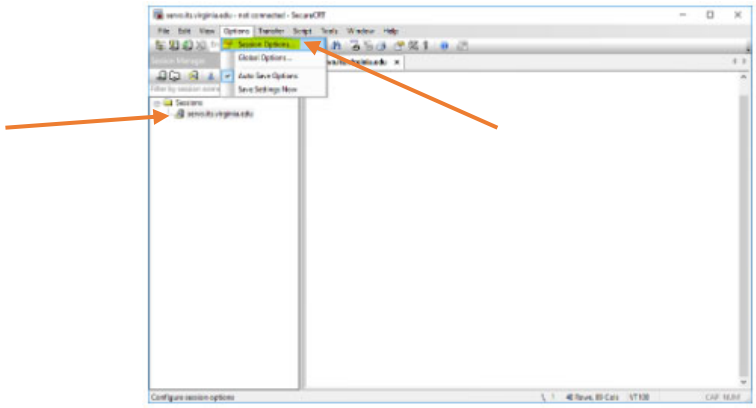
```
Your identification has been saved in /Users/mst3k/.ssh/i
Your public key has been saved in /Users/mst3k/.ssh/id_rs
The key fingerprint is:
SHA256:ozfT9m5kUBKrvdCOBl14Fuwla54YhHiIAmlb5fe3gUw mst3k@
The key's randomart image is:

+---[RSA 4096]----+
|o. ..+ . .o.     |
|o...+ o ..+oo    |
|..o  o o.E=*     |
| .    ..=B*      |
|      . SOo=     |
|       o.*+.=    |
|      . * =+     |
|       o + ..    |
|           oo    |
+----[SHA256]-----+
```

4 Send your public key (id_rsa.**pub** file) to RF ITS Managed Systems: managedsystems@rfsuny.org.

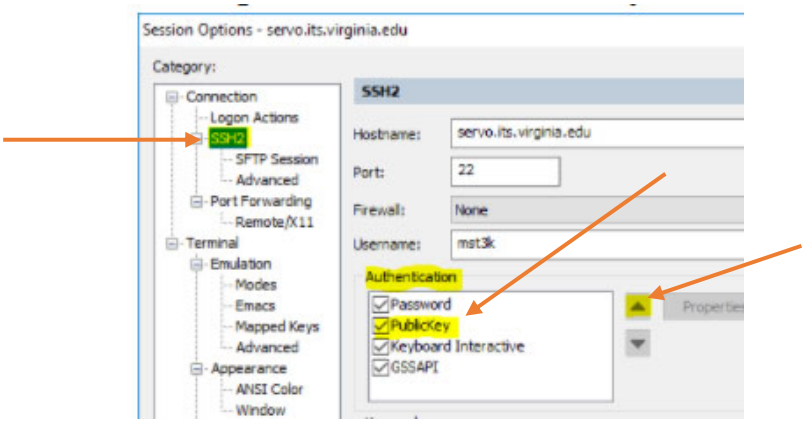
Configure Windows software to use new keys

SecureCRT

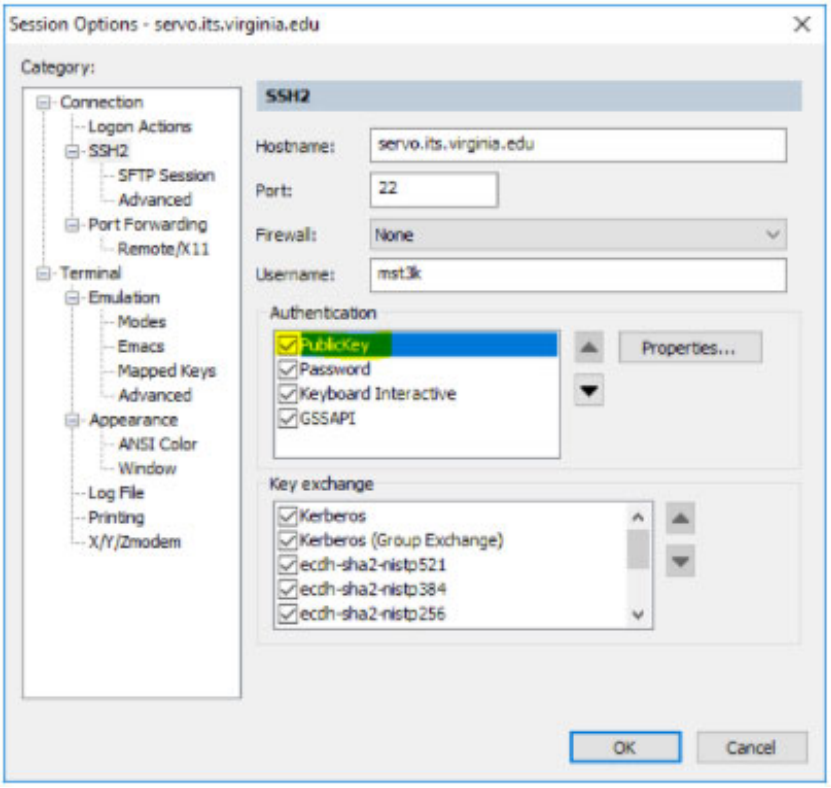
1 Select a session. Under the **Options** menu, select **Session Options.**



2 Under the **Category** sidebar, click on **SSH2**. On the right side of the window look for the **Authentication** section. Click on **PublicKey** (ensure the check remains in the box next to it). Then click on the **up arrow** on the right side of the box until **PublicKey** is at the top of the list.



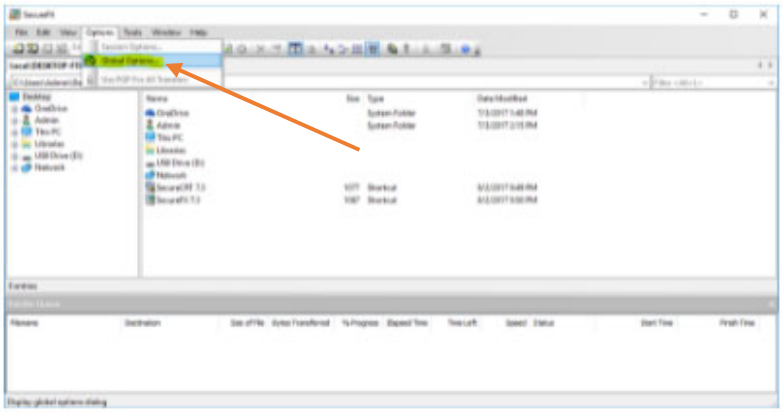
3 **When you are finished it should look like this:**



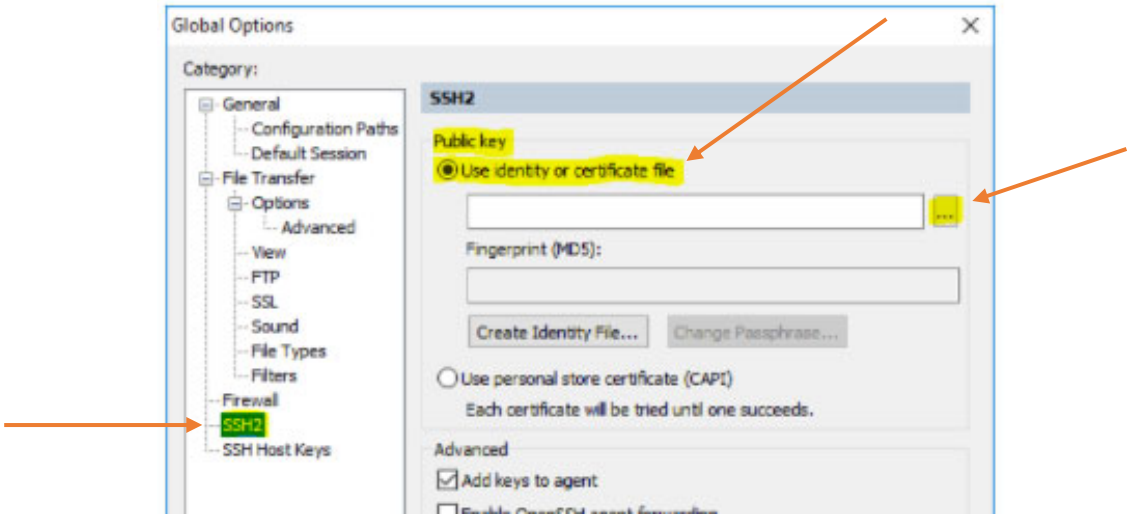
Click OK.

SecureFX

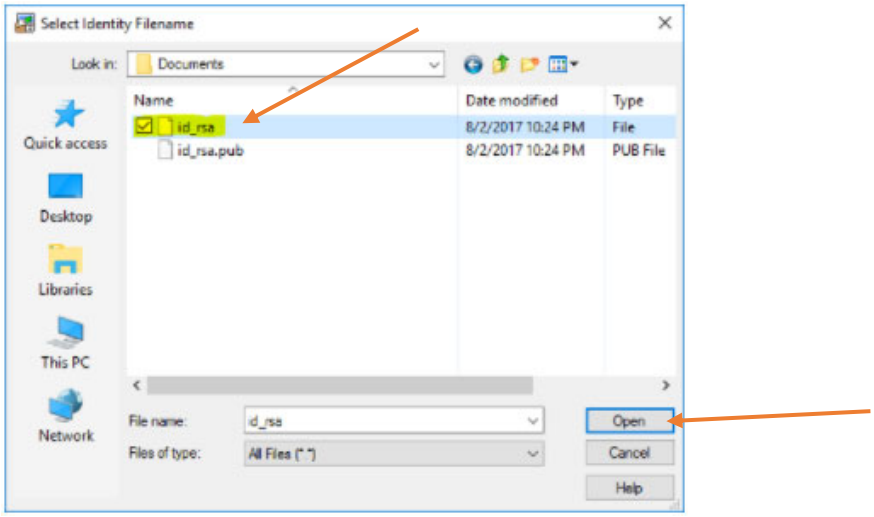
1 In the **Options** menu, select **Global Options.**



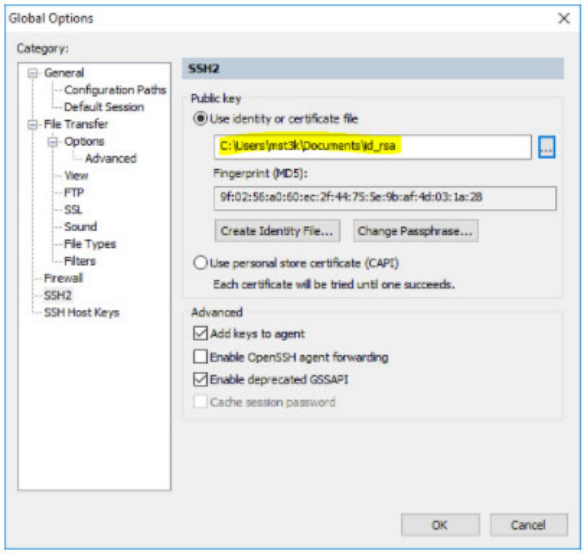
2 Under the **Category** sidebar, click on **SSH2**. On the right under **Public key**, click on the **Use identity or certificate file** radio button and then use the … button to open the **Select Identity Filename** window.



3 In the **Select Identity Filename** window, navigate to where you saved your key pair and select your private key. If you followed these instructions to create your key pair, your private key will be named **id_rsa**. Click **Open**.



4 When you are finished it should look like this:



Click **OK**.