

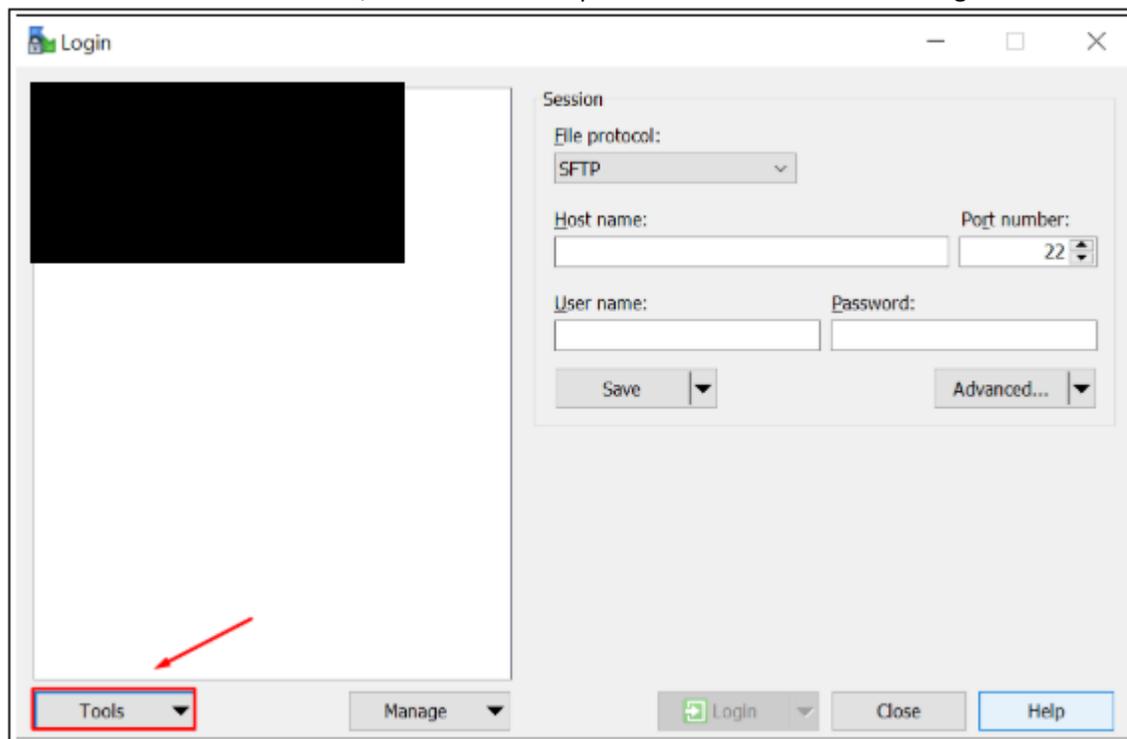
Setting Up SFTP and Creating SSH Keys

This document will walk you through the process of creating public and private key pairs. To Navigate to operating system specific instructions for creating SSH keys, please click one of the links below.

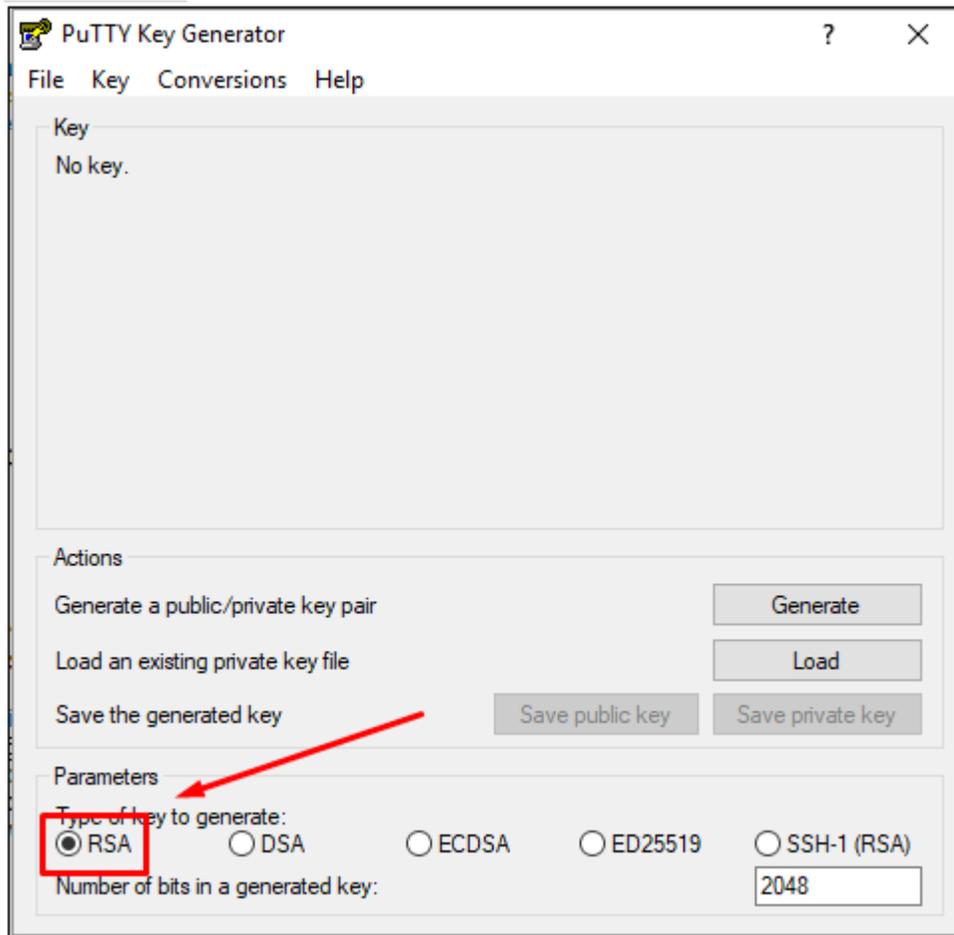
- [Creating SSH keys in Windows](#)
- [Creating SSH Keys on a Mac](#)

Creating SSH keys in Windows

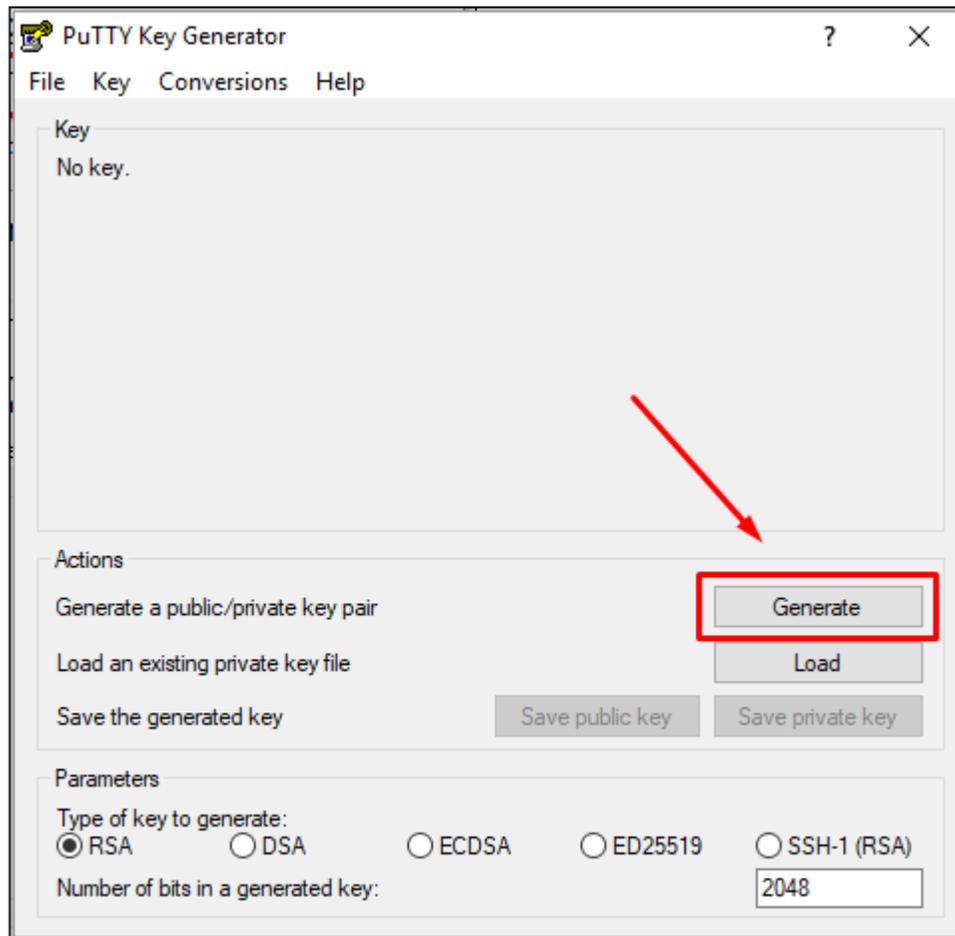
1. Download and run PuTTYGEN. PuTTYGEN is included with WinSCP, but if you're not using WinSCP, you can download a standalone version.
 - a. To run PuTTYGEN from WinSCP, click the Tools dropdown box and select Run PuTTYgen.



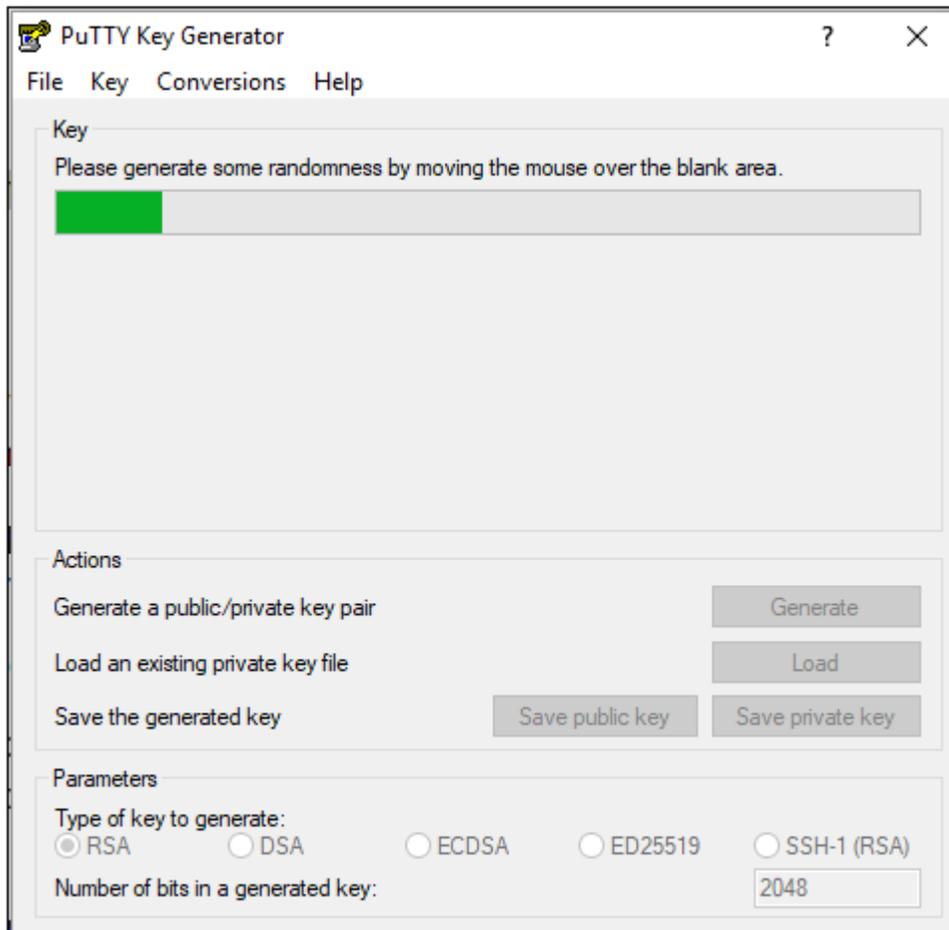
2. Select **RSA**.



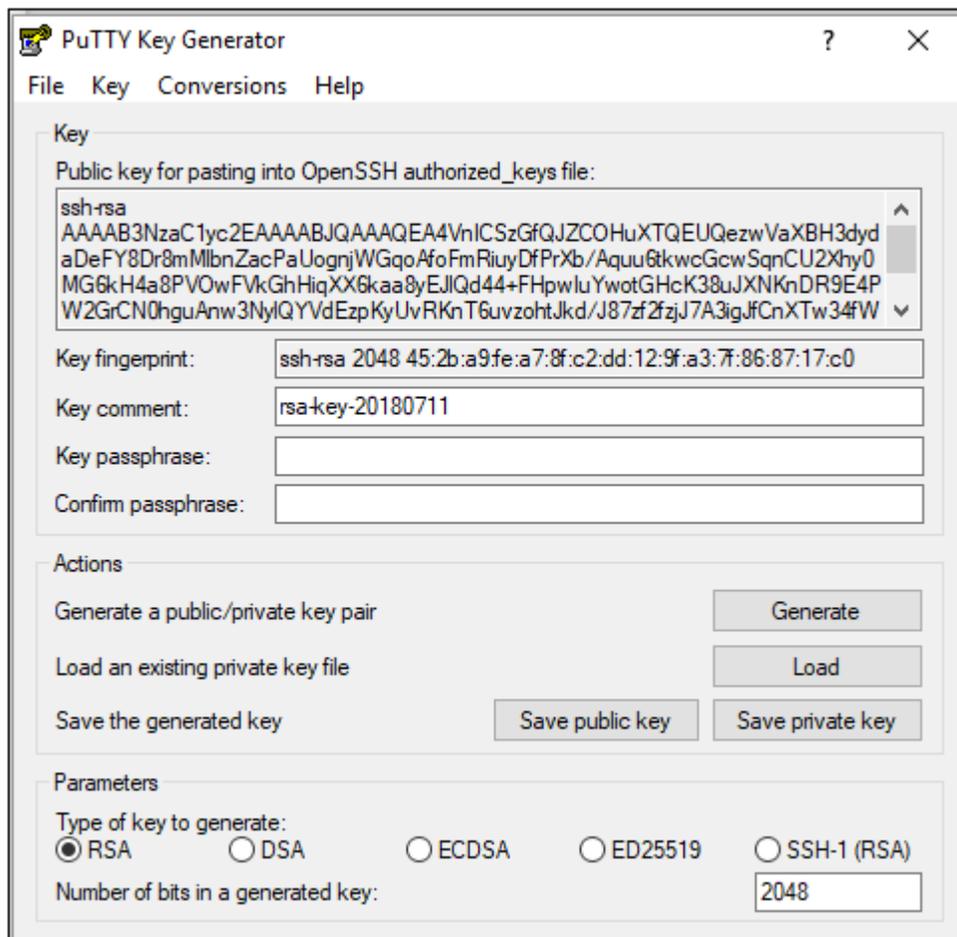
3. Click the **Generate** button.



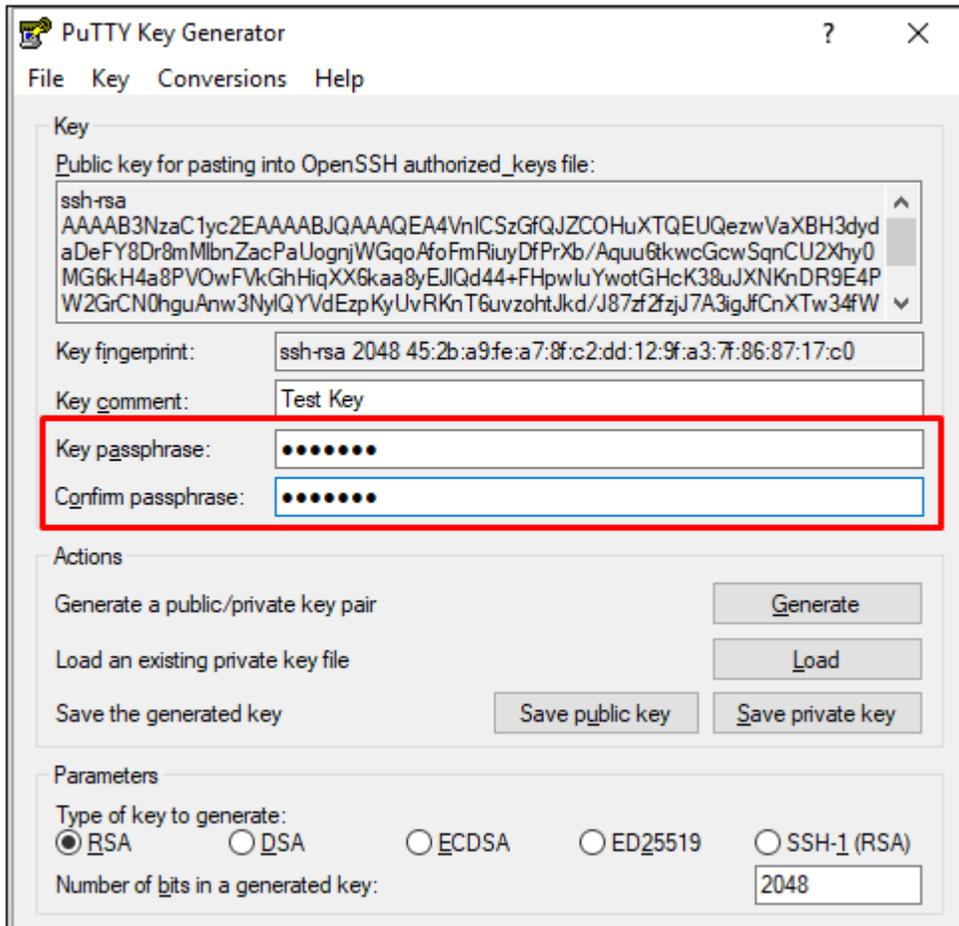
4. Move your mouse pointer around in the blank area of the **Key** section, until the progress bar is full.



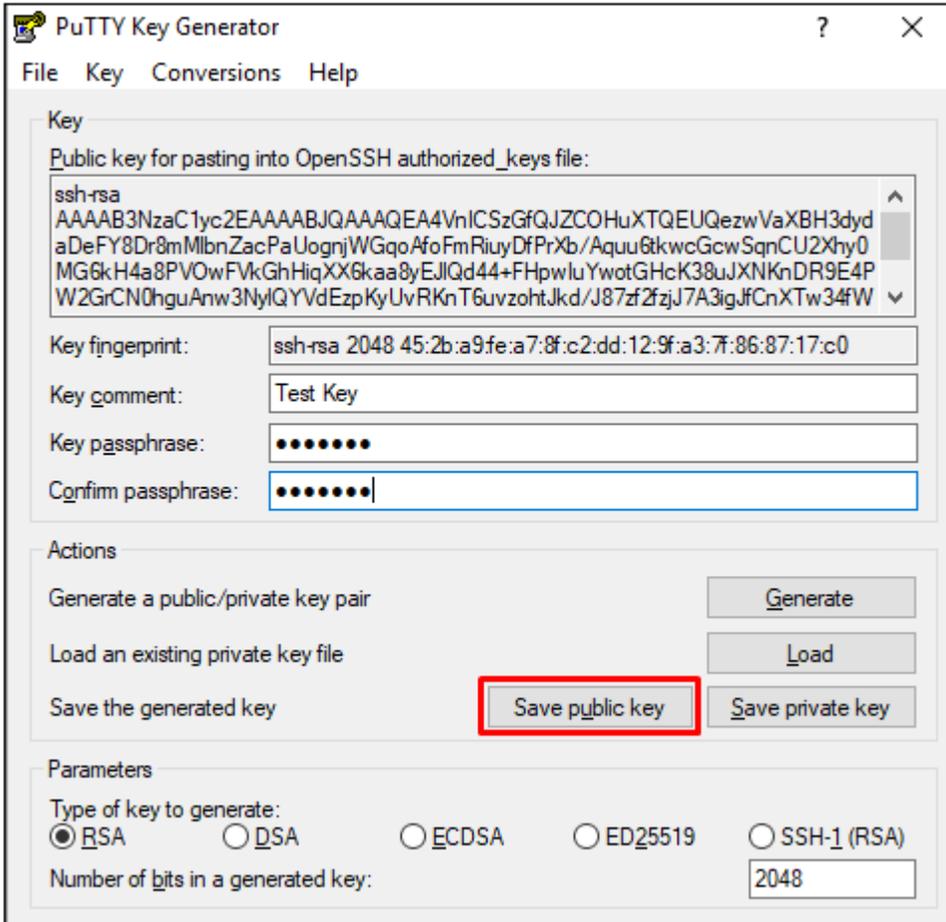
- Once the progress bar fills, the key is generated and displayed.



6. You can enter a password into the **Key Passphrase** and **Confirm Passphrase** boxes for added security but it is not required. You will have to enter this password whenever you log into the SFTP server.



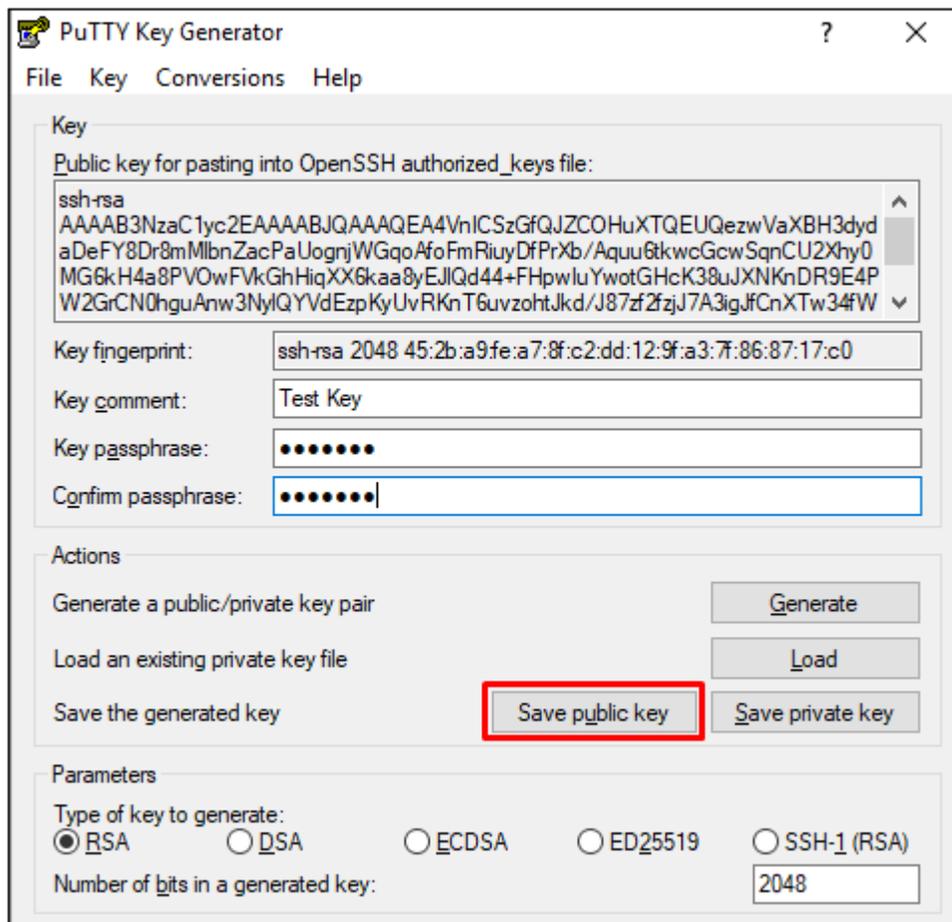
- Click the **Save public key** button and name your file. You can use any name you want, but you will want to use a descriptive name like “Conversica Public Key.”



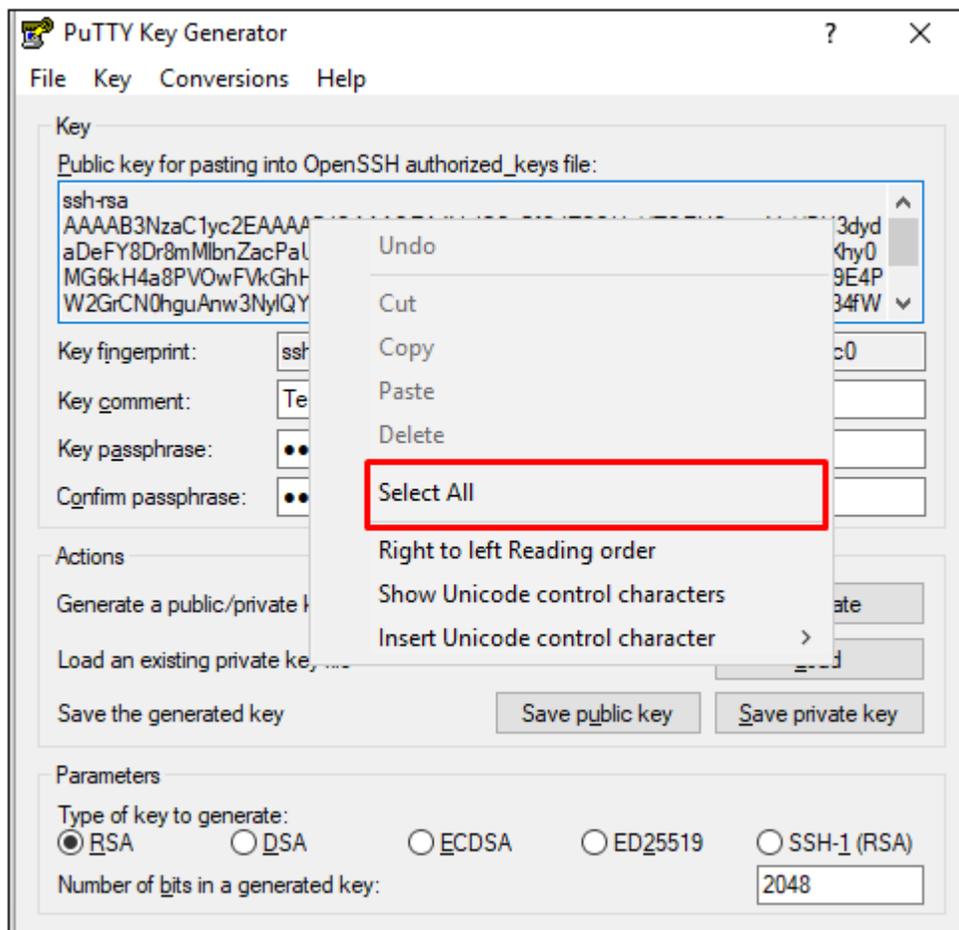
The screenshot shows the PuTTY Key Generator window. The 'Key' section contains a text area with the following public key: ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEA4VnICSzGfQJZCOHuXTQEUQezwVaXBH3dyd aDeFY8Dr8mMlbnZacPaUognjWGqoAfoFmRiuyDfPrXb/Aquu6tkwcGcwSqncU2Xhy0 MG6kH4a8PVOwFvkGhHiqXX6kaa8yEJlQd44+FHpwluYwotGHcK38uJXNKnDR9E4P W2GrC0hguAnw3NylQYVdEzpKyUvRKnT6uvzohtJkd/J87zf2fzj7A3igJfCnXTw34fW. Below this, the 'Key fingerprint' is 'ssh-rsa 2048 45:2b:a9:fe:a7:8f:c2:dd:12:9f:a3:7f:86:87:17:c0', the 'Key comment' is 'Test Key', and both 'Key passphrase' and 'Confirm passphrase' fields are filled with dots. The 'Actions' section has three buttons: 'Generate', 'Load', and 'Save public key' (which is highlighted with a red box), and 'Save private key'. The 'Parameters' section shows 'Type of key to generate' with 'RSA' selected, and 'Number of bits in a generated key' set to '2048'.

- Click the **Save private key** button and choose a file name. Make sure this private key is stored somewhere safe and it will not get lost. If something happens to this file, it will result in loss of access until a new public

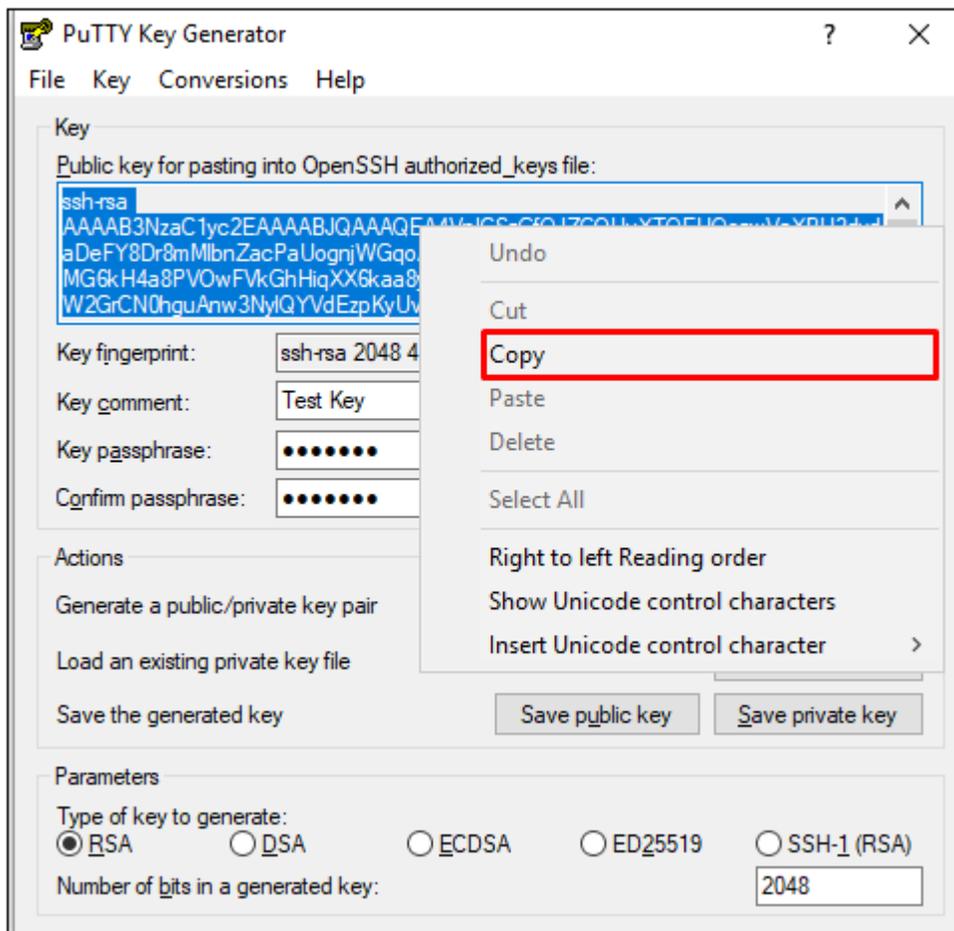
and private key pair can be made and the Conversica system can be reconfigured for the new credentials.



9. Right-click in the text field labeled **Public key for pasting into OpenSSH authorized_keys file** and choose **Select All**.



10. Right-click again once the text is highlighted in the same text field and choose **Copy**.



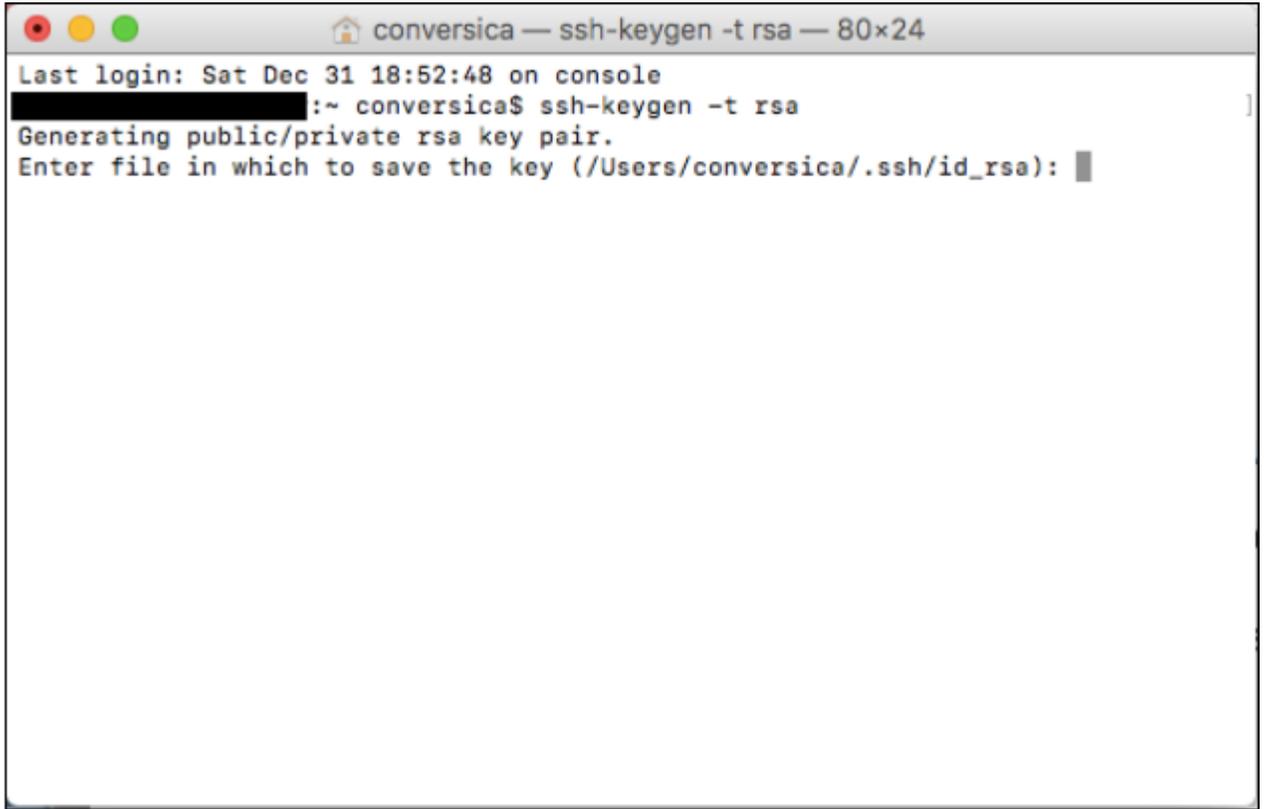
11. Send the copied value to your TAM. The key should all be on one line and begin with "ssh-rsa AAAA"

Creating SSH Keys on a Mac

1. Select **Launchpad** and type “terminal” and then click on the terminal icon.

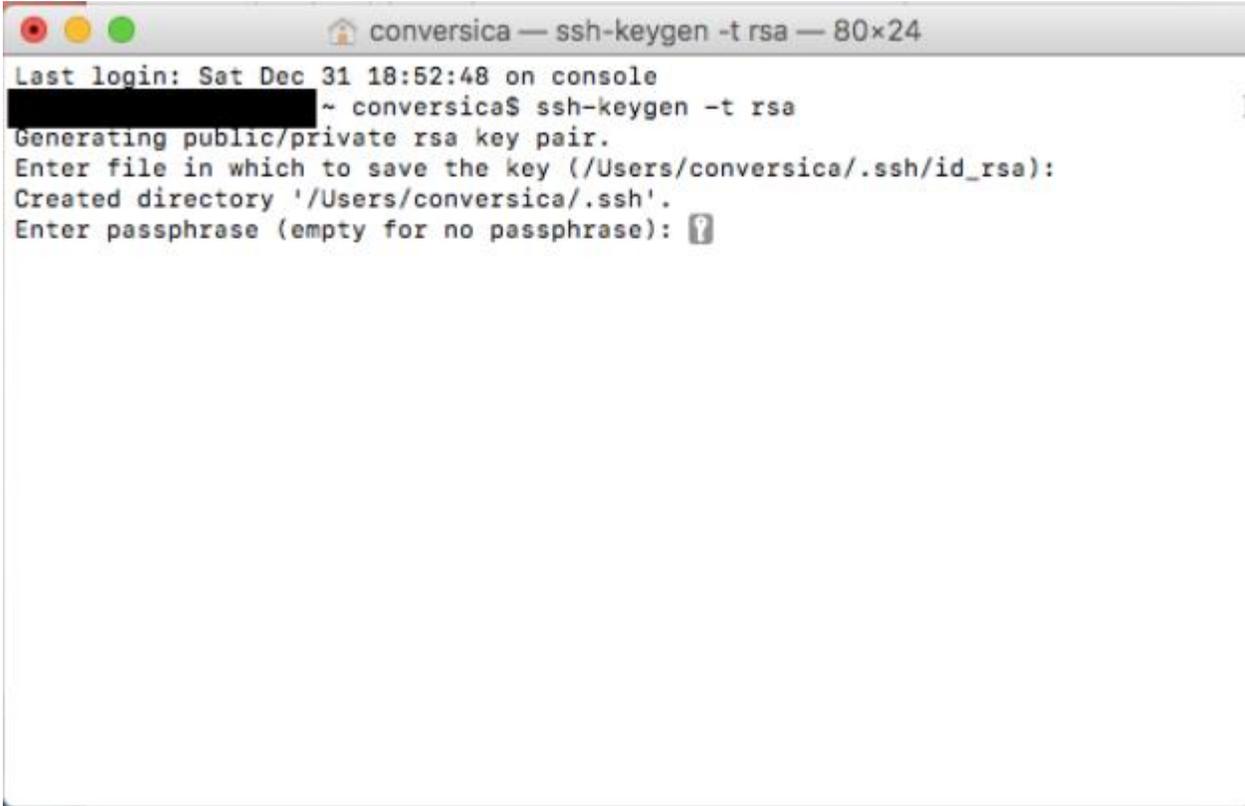


2. Type "ssh-keygen -t rsa" without the quotes.



```
conversica — ssh-keygen -t rsa — 80x24
Last login: Sat Dec 31 18:52:48 on console
[REDACTED]:~ conversica$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/conversica/.ssh/id_rsa):
```

3. You will be prompted for a location to save the key files. If you just press Enter it will save in the default location. The rest of these instructions are written as though you saved to the default location.



```
conversica — ssh-keygen -t rsa — 80x24
Last login: Sat Dec 31 18:52:48 on console
~ conversica$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/conversica/.ssh/id_rsa):
Created directory '/Users/conversica/.ssh'.
Enter passphrase (empty for no passphrase):
```

4. You will be prompted for a passphrase. You can enter one or leave it empty. If you enter a password, you will need to enter it twice and the passphrase will need to be entered every time you log into the SFTP directory.

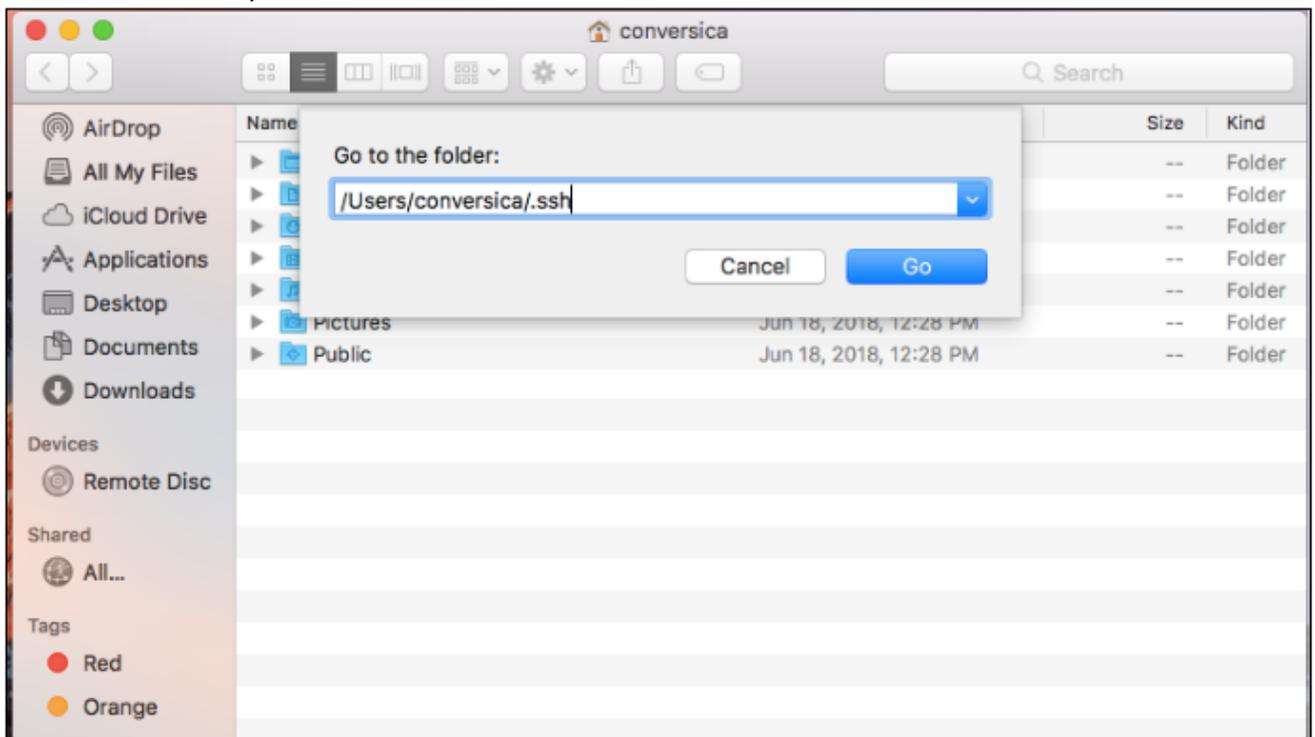
- Terminal will display a message giving the location of the new files and it will provide a key fingerprint and random art. You do not need the fingerprint or random art.

```

conversica — -bash — 80x24
[redacted]:~ conversica$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/conversica/.ssh/id_rsa):
Created directory '/Users/conversica/.ssh'.
[Enter passphrase (empty for no passphrase):
[Enter same passphrase again:
Your identification has been saved in /Users/conversica/.ssh/id_rsa.
Your public key has been saved in /Users/conversica/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:hCVV1xniUCYocsBYCVScB7f/iK6BPK4GgUYdxPhsg+E conversica@BrianKs-MacBook-Ai
r.local
The key's randomart image is:
+---[RSA 2048]-----+
|o*XB+..o=o= o+
|.++++.o+ = oo
|+ =o.o. . .
|oE = ..
|... . .S
|o . . o
|. + . . . .
|... o
|. + . . .
+---[SHA256]-----+
[redacted]:~ conversica$

```

- Press **Command + Shift + G** and enter the location that terminal says the file was stored to go to the location where the key file was saved.



7. Copy the .pub file to an email and send it to your TAM.

You are now ready to log into your directory. Please contact your TAM for the next steps.