SSH Key Pair Generation

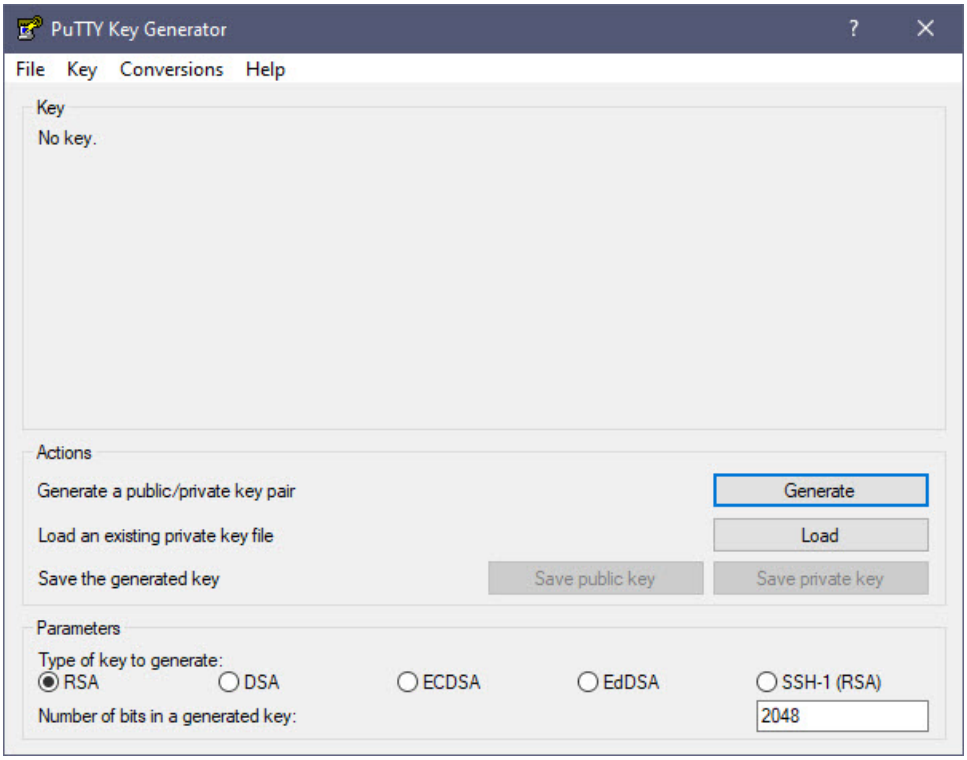
Managed File Transfer (MFT)

The PuTTY Key Generator application (putygen.exe) is a free downloadable application you can use to create a new SSH key pair consisting of a private and public key. These keys function as the password when signing on to the BOKF MFT environment using the SFTP protocol. Follow these simple instructions on how to use PuTTY Key Generator to create a new SSH key pair for use with your BOKF MFT account.

You can download the **putygen.exe** by copying and pasting this URL into your browser https://www.chiark.greenend.org.uk/%7Esgtatham/putty/latest.html.

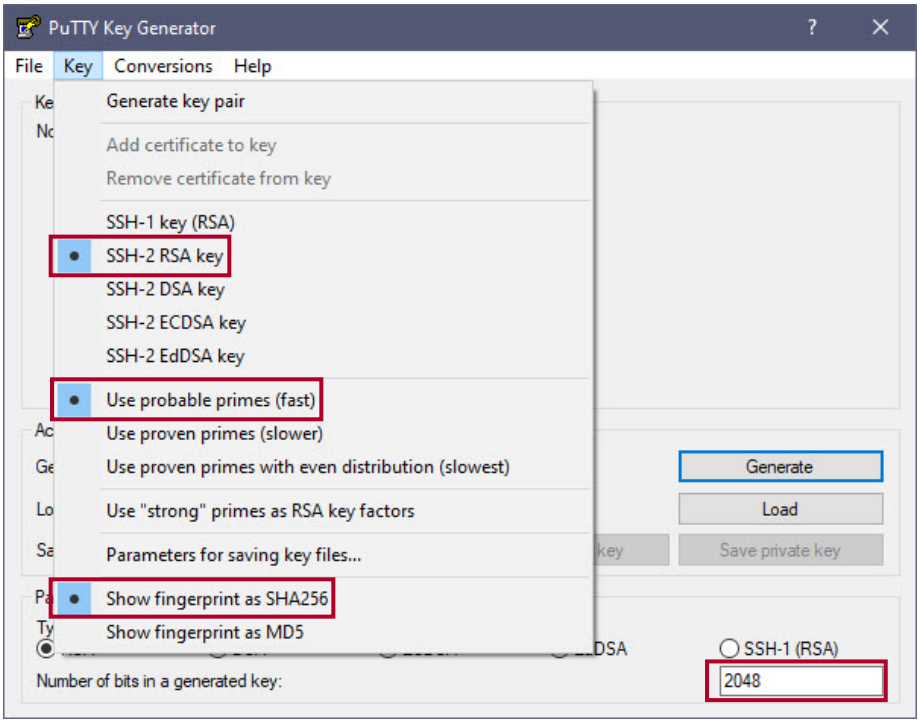
1. Once you have downloaded the **putygen.exe** executable, navigate to the folder where you saved the downloaded file.

2. Double-click the **putygen.exe** executable to launch the application. Once open, it should appear as it does here.

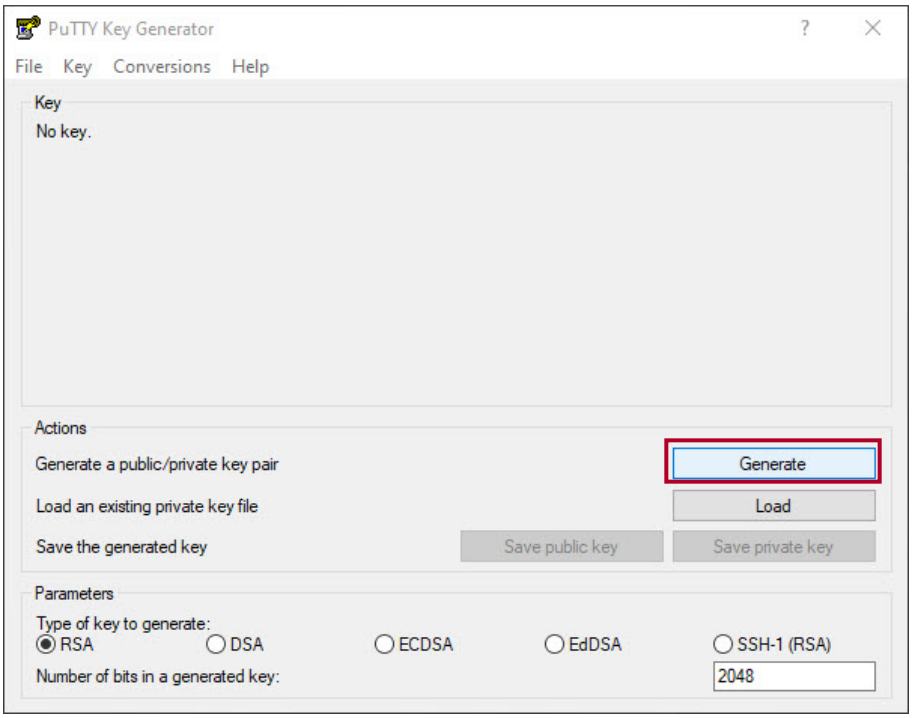


3. Click “Key” from the menu to view the current configured settings. If different than what is show here, match your settings as these are the most common used.

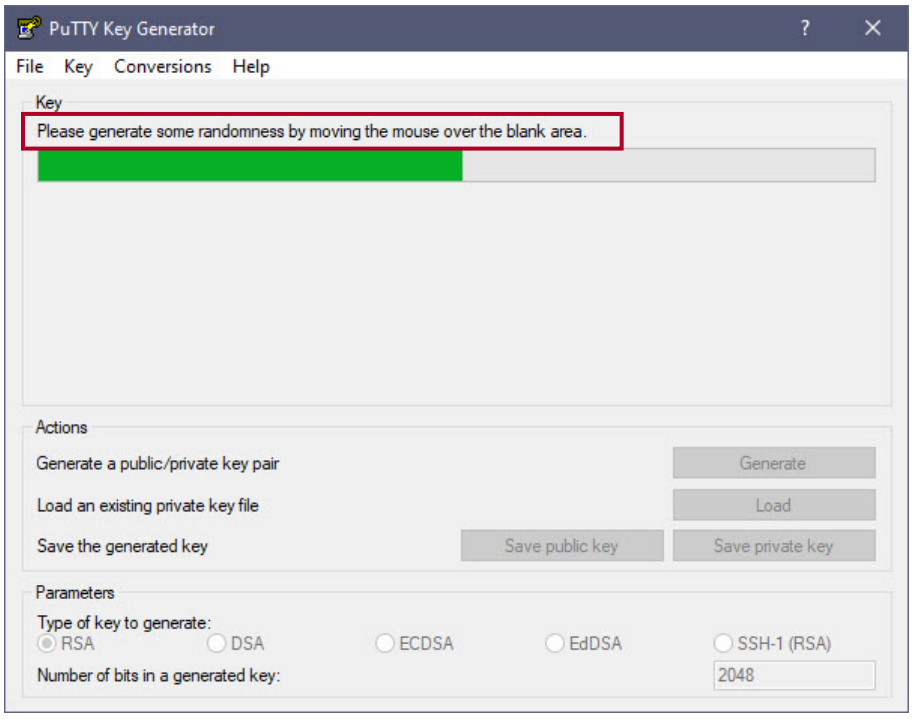
4. You can also set the “Number of bits in a generated key.” The default is **2048** bits. You could go to a stronger **4096** bits, but it is not necessary.



5. Now that your **Key** has been set and you have picked the number of bits to be generated in the key (2048 or 4096), click the “Generate” button to begin the **RSA** key generation process.

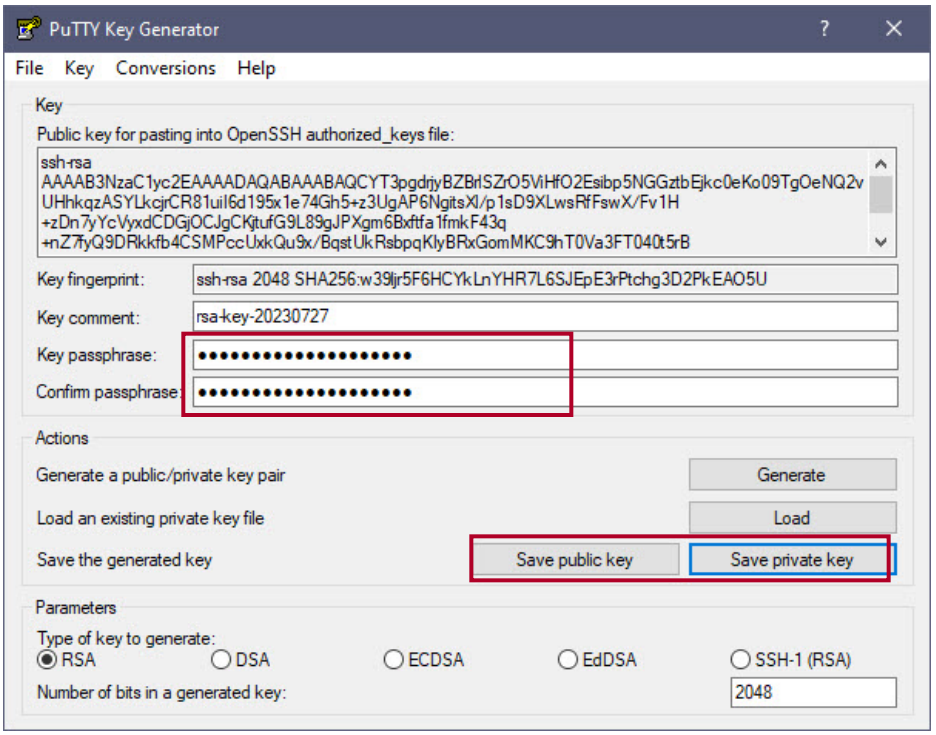


6. When the key generation process starts, you will be prompted to “generate some randomness.” This is done by moving your mouse cursor around on your screen in random patterns. As you do this, you will see the green progress bar grow.

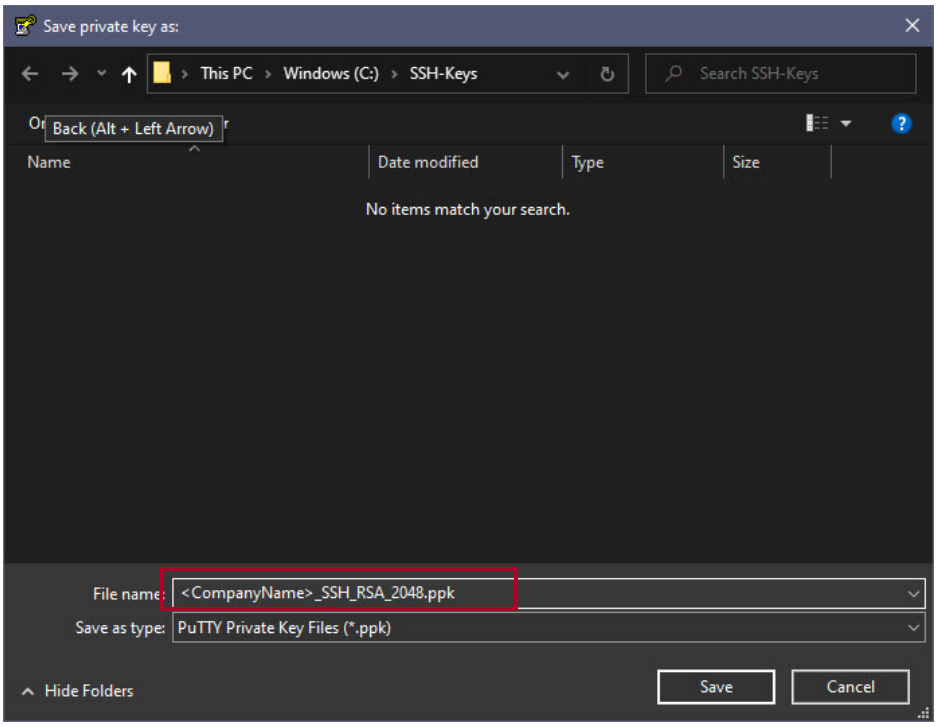


7. Once the key generation is complete, you will see information like what is shown here. Enter a “Key passphrase” and “Confirm passphrase”. This secures your private key and ensures that no one else can use it. You will want to record the passphrase (password) in a password vault or wherever passwords are stored.

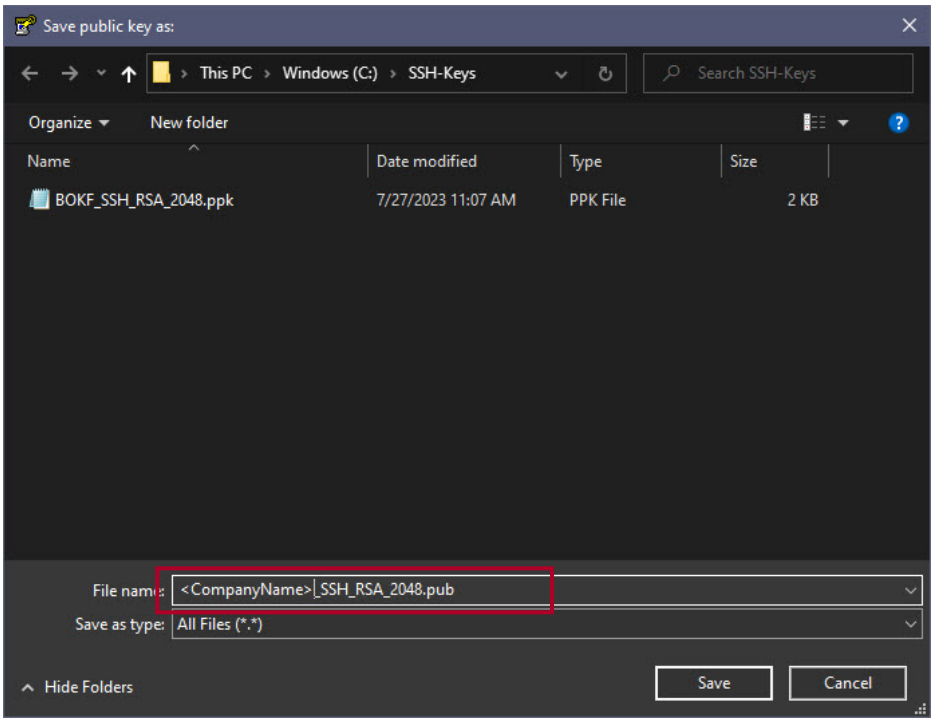
8. Next, save both your “private” and “public” keys somewhere safe.



9. When you save your private key, it should have a **.ppk** file extension. Including some details in the filename will help you in the future.



10. When saving your public key, you will need to specify the file extension **.pub** at the end of the filename.



11. You should now have an SSH key pair consisting of one private key and one public key. You will configure your client to use the private key with your BOKF MFT user ID. You will need to provide the public key to BOKF so it can be imported into the MFT environment and tied to your account for authentication.