Creating and Using SSH Keys

The Secure SHell (SSH) protocol is used to securely access remote servers. SSH secures information with the use of a private and public key. The public key is like a lock, anybody can see it but only the person with the private key can unlock it. So when you connect to the remote server, the server confirms your identity by seeing if your private key unlocks the lock. This checking continues as information is sent to you from the server. The private key should be kept private (hence the name); anybody who has the private key can impersonate the person who generated it and steal their private information.Not only do SSH keys help to protect your data, they add convenience. Instead of entering your RIT password (which you have to change at least once a year) every time you SSH into a remote machine, you can enter the passphrase for a private ssh key (which you never *have* to change).

Key Generation and Set up with Linux / Mac / Windows with MobaXterm

1. Open the terminal on your computer
2. In the command line run:
   ```
   ssh-keygen -t rsa
   ```
3. The terminal will respond with:
   ```
   Generating public/private rsa key pair.

   Enter file in which to save the key ( /home/RITusername/.ssh/id_rsa):
   ```

   Hit enter to continue
4. Next it will prompt you to enter a passphrase and confirm it. Do not leave it empty:

   ```
   Enter passphrase (empty for no passphrase):

   Enter the same passphrase again:
   ```
5. Now it will tell you where your key pair was saved:

   ```
   Your identification has been saved in /home/username/.ssh/id_rsa

   Your public key has been saved in /home/username/.ssh/id_rsa/pub
   ```

   The identification is your private key. You can open these files in a text editor and see the keys. The fingerprint of the key and it's randomart image is also displayed. These are used to help recognize keys.
6. To add the key to the remote server run:

   ```
   [abc1234@computer ~] ssh-copy-id -i .ssh/id_rsa.pub abc1234@computerhost.rit.edu
   ```

   *If the ssh-copy-id command is not available on your machine,skip the following steps and go to the Alternative to ssh-copy-id heading.
7. The terminal may show you the key fingerprint and ask if you still want to install it. Type yes.
8. Next the terminal will ask you to enter your password for the remote machine.
9. Now the terminal will say that a key was added and ask you to try logging into the machine you just copied the public key to. If all is right you will not have to enter your RIT password, but instead the passphrase for the key generated.
10. To circumvent entering your passphrase every time you SSH into a machine, you can use the ssh-agent command that will enter the passphrase for you. See the Using ssh-agent heading.

Alternative to ssh-copy-id

The ssh-copy-id command may not be available on older versions of the Mac OS. To install this command on your Mac follow the instructions provided here: https://www.ssh.com/ssh/copy-id#sec-Ssh-copy-id-on-Mac.

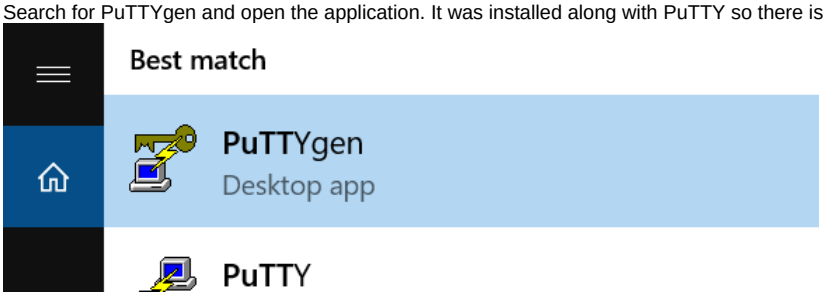
If you do not want to or cannot install the shh-copy-id command use this alternative. It does the same thing as ssh-copy-id.

1. Run this command in your terminal:

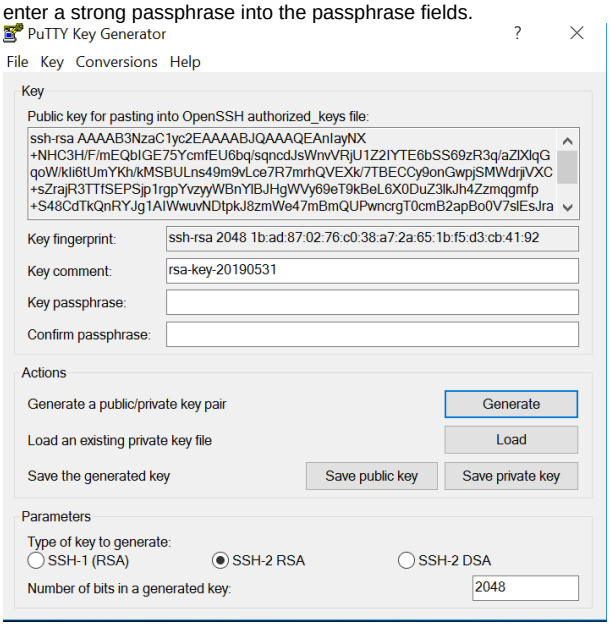
   ```
   [abc1234@computer ~] cat ~/.ssh/id_rsa.pub | ssh abc1234@computerhost.rit.edu "cat - >> ~/.ssh
   /authorized_keys"
   ```
2. You will then be prompted to enter your RIT password for the remote machine.
3. Next time you log into the remote machine you will be prompted to enter the passphrase for the private key and then you will be able to access the machine.

Key Generation and Setup on Windows with PuTTY

1. Search for PuTTYgen and open the application. It was installed along with PuTTY so there is no need to download it.



2. Leave all the settings as they are and click Generate. You will be asked to move your mouse around the area to generate randomness. After, enter a strong passphrase into the passphrase fields.



3. Save the public key as id_rsa.pub somewhere on your computer. These keys can be named anything you want, id_rsa is just the default when generating from the command line.
4. Save the private key as id_rsa.ppk somewhere safe on your computer. Do not share this file with others. Do not close out of this window.
5. Use PuTTY to SSH into the remote machine.
6. If the .ssh file has not been created:

```
mkdir ~/.ssh

chmod 700 ~/.ssh
```

7. If the authorized_keys file does not exists:

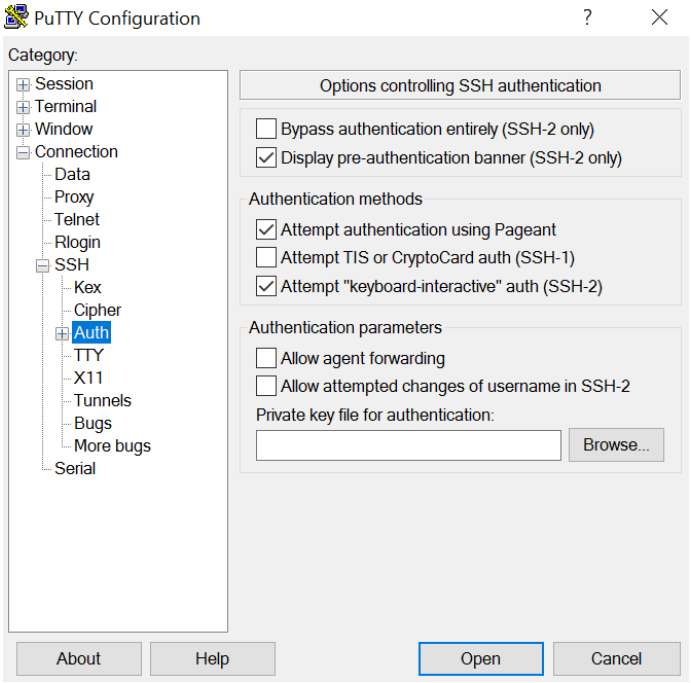
```
touch ~/.ssh/authorized_keys

chmod 600 ~/.ssh/authorized_keys
```

8. `Open the authorized_keys file with a text editor of your choice:`

```
vim ~/.ssh/autorized_keys
```

9. Copy the public key from the PuTTYgen window and paste it to the end of the authorized_file. The way PuTTYgen saves their public keys is not compatible with the authorized_keys format so you cannot copy and paste from the public file itself. You must open it from the PuTTYgen window by clicking Load, selecting the corresponding private key, and entering the passphrase.
10. Save the authorized_key file and log out of the terminal.
11. Open PuTTY again and in the menu to the side of the window navigate to Connection SSH Auth



12. Click Browse and find where you stored the private key that corresponds to the public key you just pasted into authorized_keys.
13. Go back to the Session tab and enter information as you would regularly.
14. When the terminal is open it will say:

    ```
    Authenticating with public key “rsa-key-######”

    Passphrase for key “rsa-key-#####”
    ```

15. Enter the passphrase for the key and you are set.

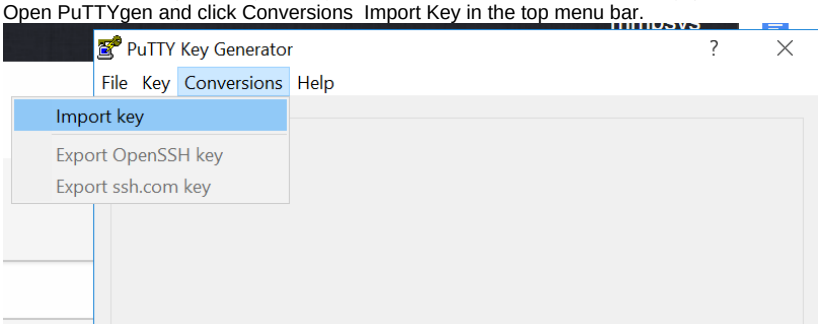
To avoid entering your passphrase every time you use PuTTY for SSH, you can use PuTTY's Pageant. Instructions for Pageant are under the Pageant and Desktop FastX heading.

FastX Web Client

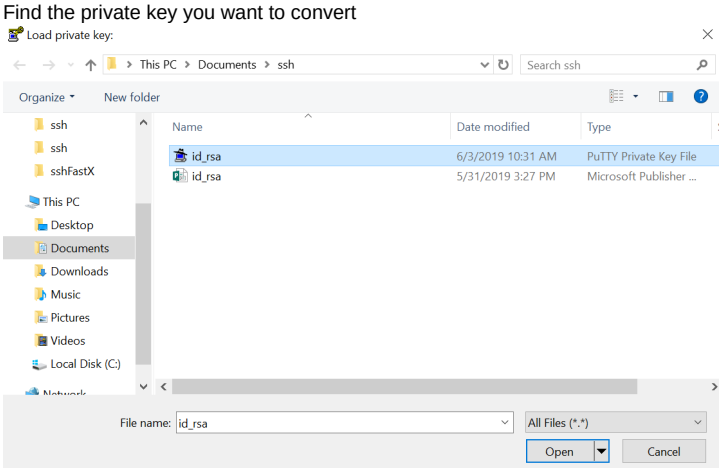
Windows with PuTTY Setup

FastX does not support PuTTY's format for private SSH keys, so we need to first convert them into OpenSSH format.

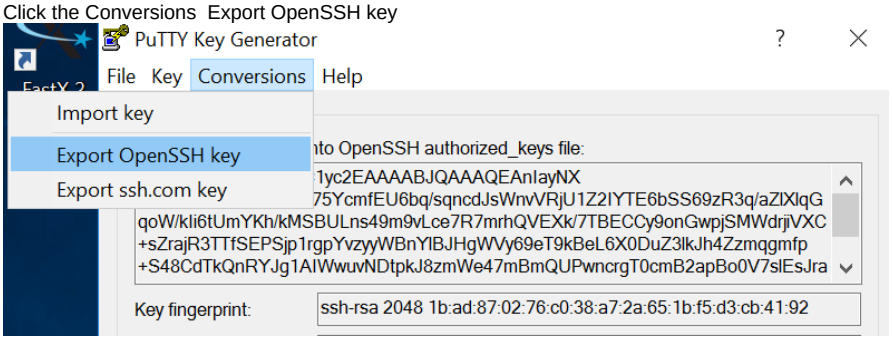
1. You must have the public key already on the remote machine. Follow the key generation and setup instructions for Windows with PuTTY.
2. Open PuTTYgen and click Conversions Import Key in the top menu bar.



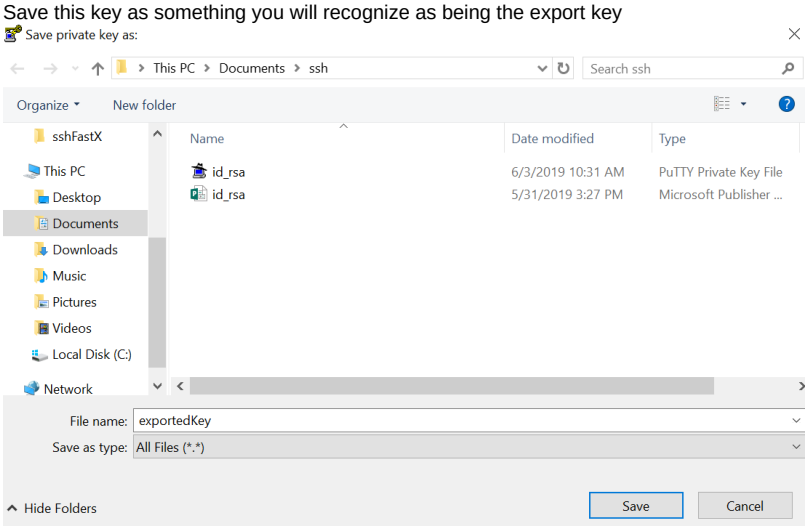
3. Find the private key you want to convert



4. Enter the passphrase for the key
5. Click the Conversions Export OpenSSH key



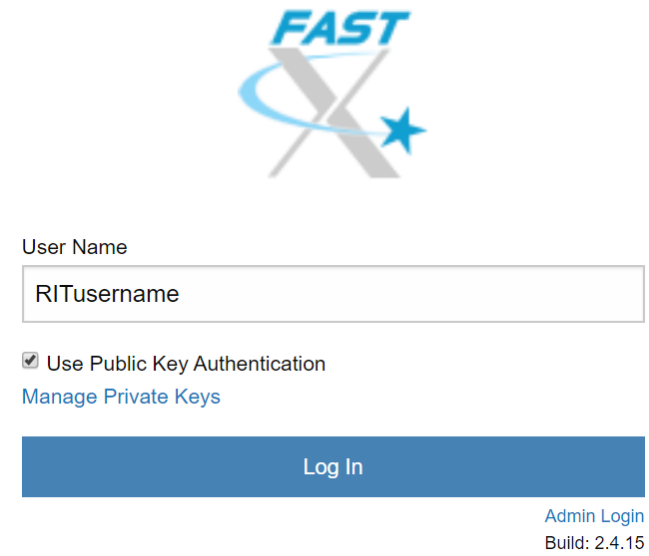
6. Save this key as something you will recognize as being the export key



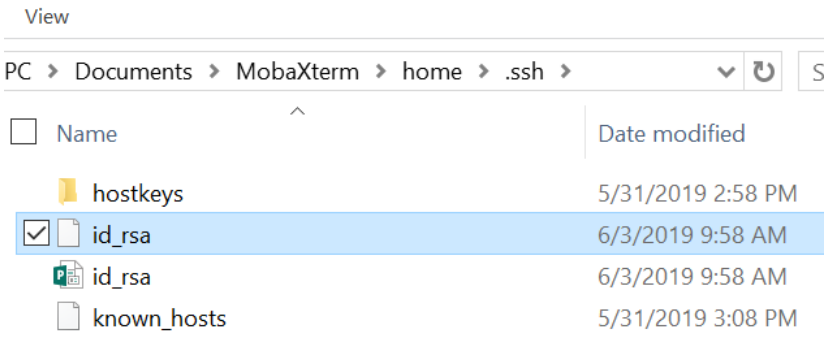
7. You can exit the PuTTYgen window

Now we are ready to use SSH keys with FastX

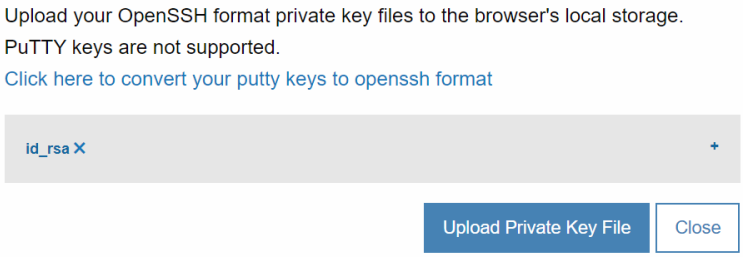
1. Go to the FastX login screen for the remote machine you want to login to. Enter your username and check ‘Use Public Key Authentication’.



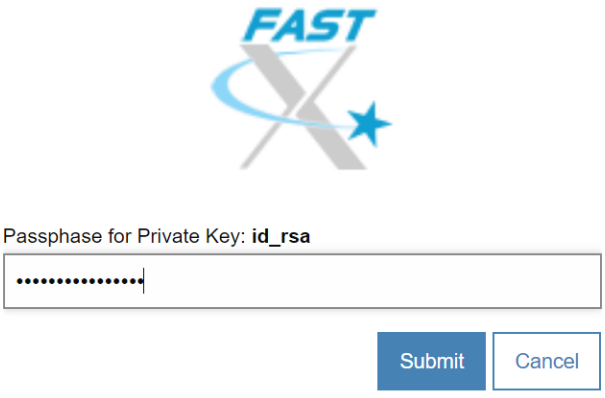
2. Navigate to where the private key is stored and select it.



3. Click close



4. Click Login. You will be prompted to enter the passphrase for the private key.



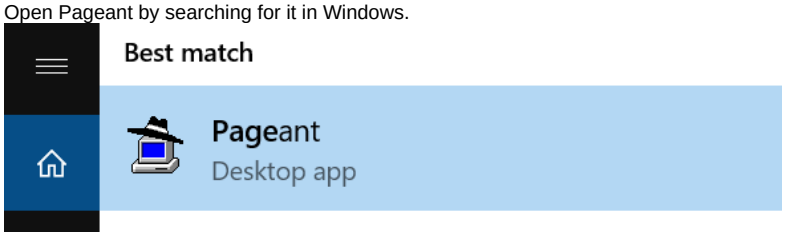
5. The first time you use the key you will be prompted to enter your RIT password.

6. Now that you have connected with the key once, the next time you connect you will only be prompted for the key's passphrase.

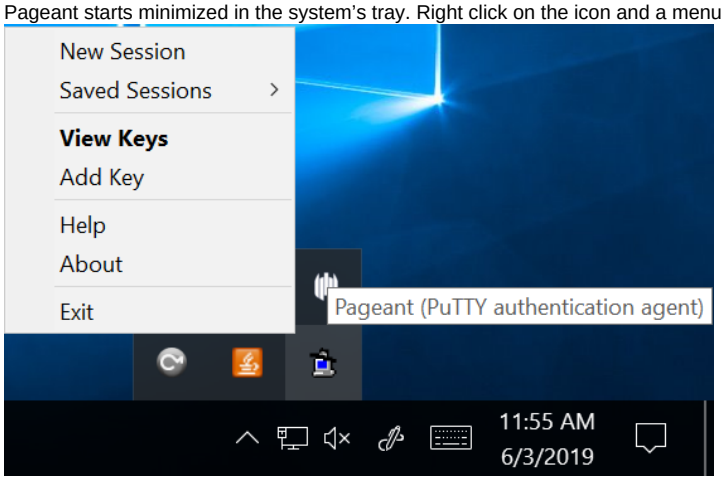
Using Pageant (Windows)

Pageant is a tool included with PuTTY that runs as a background process and enters the passphrase for the private keys for you. If you are using MobaXterm you cannot use the key generated by ssh-keygen, you must use the generator which is found under Tools MobaKeyGen. MobaKeyGen is ver y similar to PuTTYgen, so you can use the instructions under Key Generation and Set up on Windows with PuTTY.

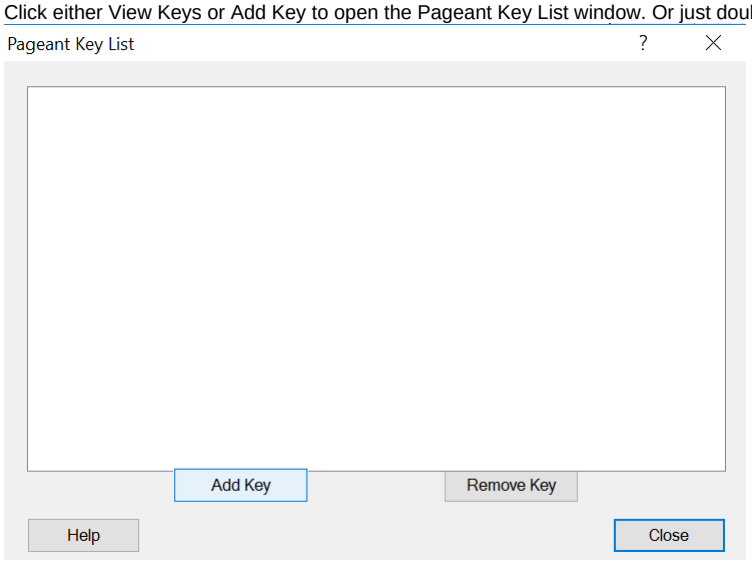
1. First you must have the public key in the authorized_keys file on the remote machine. Follow the instructions for Key Generation and Setup on Windows with PuTTY.
2. Open Pageant by searching for it in Windows.



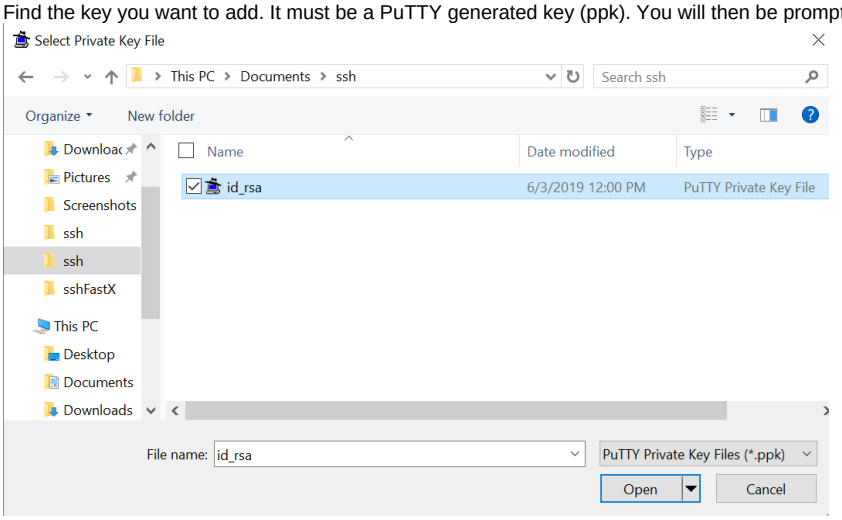
3. Pageant starts minimized in the system's tray. Right click on the icon and a menu will appear :



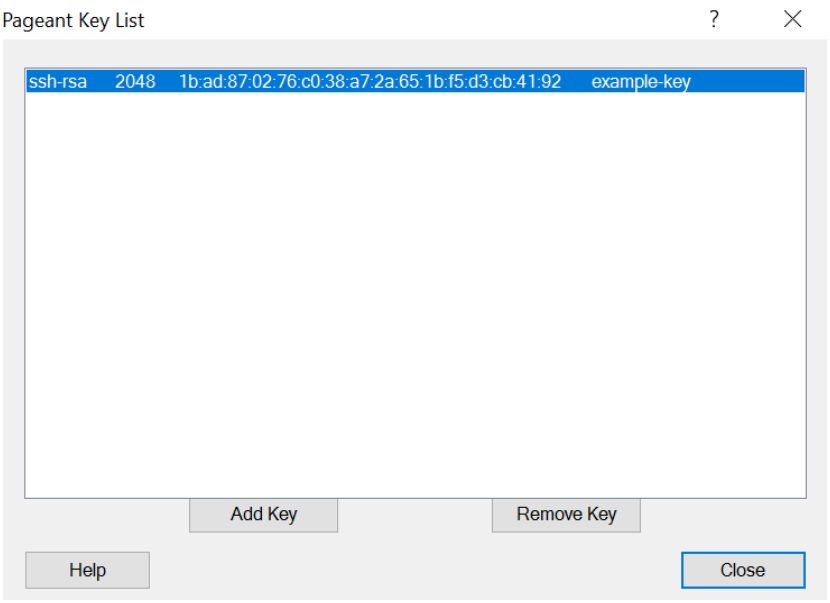
4. Click either View Keys or Add Key to open the Pageant Key List window. Or just double-click the icon in the tray. To add a key press Add Key.



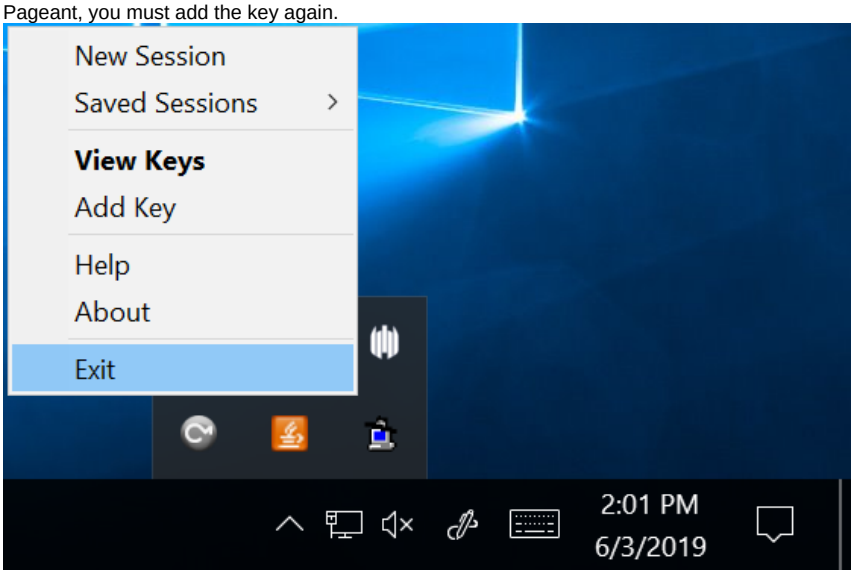
5. Find the key you want to add. It must be a PuTTY generated key (ppk). You will then be prompted to enter the passphrase for the private key.



6. Now the key is loaded into Pageant.



7. Now if you use PuTTY with SSH keys you will not have to find the private key or enter the passphrase.
8. Make sure when you are done using SSH to log into the remote machines you right click the Pageant Icon and click Exit. The next time you open Pageant, you must add the key again.



Using ssh-agent (Mac / Linux / MobaXterm)

The ssh-agent is a background process that automatically enters the passphrase for private keys. You must have at least one key already set up on your computer. Follow the instructions under Key Generation and Set Up with Linux / Mac / MobaXterm to do this.

1. Open your terminal and starting the program by running:
   `eval \`ssh-agent\``

   Note: Backquote (`) is located under tilde (~), the backquote is not a single quote (')
2. Next add the private key to the agent:
   `ssh-add`
3. You will then be asked to enter the passphrase for the private key.
4. Now you can connect through FastX as you normally would without entering your RIT password or passphrase for the private key.
5. When you are done using FastX and SSH into the terminal type:
   `kill $SSH_AGENT_PID`
   You can add this command to your .bash_logout file (for bash users) or .logout (for csh or tcsh users) so that it happens automatically when you log out.

FastX Desktop Client and SSH Keys

You can use SSH keys on FastX as well. When you use the keys with FastX, you will not have to enter your RIT password or your passphrase. This is because you will be using Pageant or ssh-agent that enters the keys for you. Simply have ssh-agent or Pageant running in the background while you run FastX. Make sure to end those processes when you are done with FastX.

If there are any further questions, or there is an issue with the documentation, please contact rc-help@rit.edu *for additional assistance.*