**How to set up RSA Key Authentication**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Client Machine to Remote Server Authentication (PuTTY)**

1. ssh-keygen

From the Command Prompt on your local machine, enter the following command:

C:\> ssh-keygen

Press Enter through the prompts - do not create a passphrase for your key. This should create two files in *C:\Users\<your name>\.ssh*:

*id\_rsa* - your private key

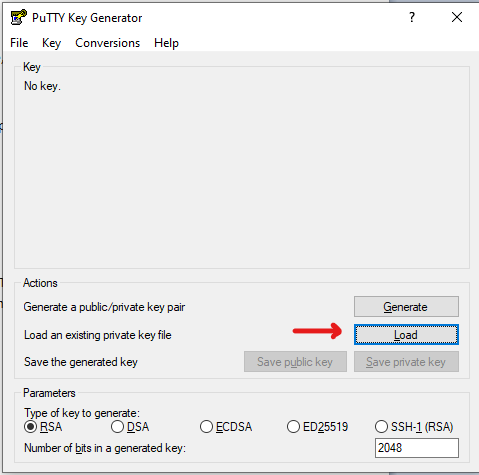
*id\_rsa.pub* - your public key

2. puttygen.exe

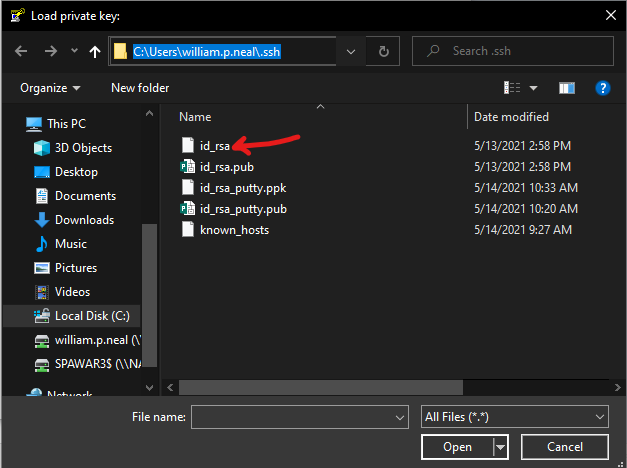
In order to use key authentication with PuTTY, you must use puttygen.exe. If your PuTTY folder is added to %PATH%, you can launch puttygen.exe from the command line:

C:\> puttygen

From the puttygen window, select "Load".



In *C:\Users\<your name>\.ssh* select the *id\_rsa* file.



This will create a "putty version" (.ppk) of your OpenSSH private key. I named mine id\_rsa\_putty.

3. add .pub to .ssh/authorized\_keys

From the Command Prompt, cd to the *.ssh* directory

C:\> cd C:\Users\<your\_name>\.ssh

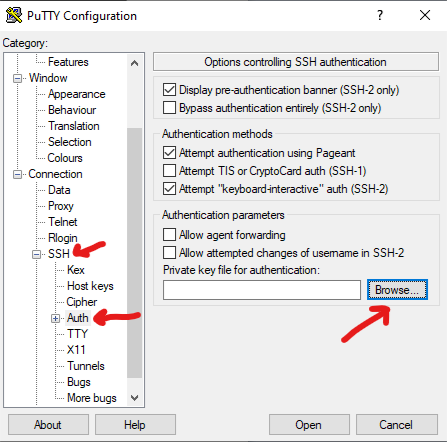
and run the following command:

C:\> type id\_rsa.pub | ssh <your login>@<hostname> "mkdir .ssh && cat >> ~/.ssh/authorized\_keys"

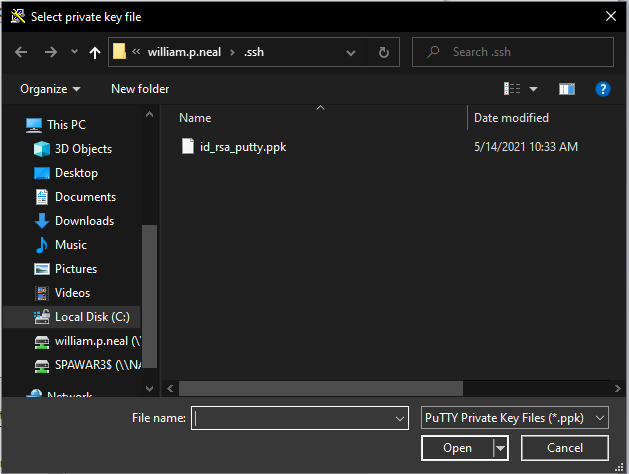
Enter your password at the prompt. This will create the *.ssh* directory on the server and write your public key data into the *authorized\_keys* file. Note: The *.ssh* directory chmod permissions should be 700 and the *authorized\_keys* file should be 600.

4. update putty SSH settings

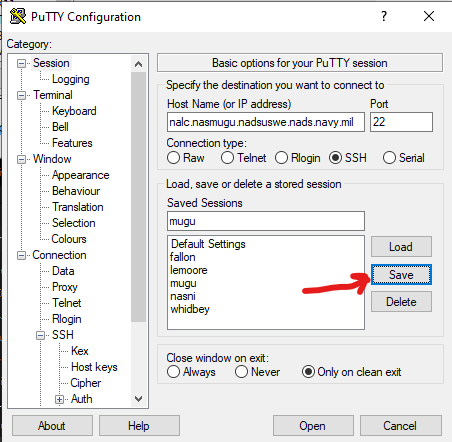
Open PuTTY and load the your saved session for the server your pushed your public key to. Then go to the menu Connection>SSH>Auth, and select the Browse button.



Select the .ppk file you created in step 2.



Save the session settings, and launch the session. Putty should now log your into the server without requested a password.



The same key pair can be used for every site, simply repeat steps 3 and 4 for each site you wish to use key authentication for. If you already have a .ssh directory on the server, use:

C:\> type id\_rsa.pub | ssh <your login>@<hostname> "cat >> ~/.ssh/authorized\_keys"

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Remote Server to Remote Server Authentication (SSH)**

1. ssh-keygen

From your account on the server, enter the following command:

$ ssh-keygen

Press Enter through the prompts - do not create a passphrase for your key. This will create two files in */h/USERS/<your name>/.ssh2*:

*id\_rsa\_2048\_<hostname>* - your private key

*id\_rsa\_2048\_<hostname>.pub* - your public key

2. Convert SSH2 keys to OpenSSH format

Running ssh-keygen on the NTCSS servers will generate keys in the SSH2 format, the public key needs to be converted to OpenSSH format to work. To do this, run the following from *~/.ssh2*:

$ ssh-keygen -H id\_rsa\_2048\_<hostname>.pub

This will create a file called *id\_rsa\_2048\_<hostname>.pub.ssh* containing your public key in OpenSSH format.

3. Add identification file and IdKey

From the .ssh2 directory, run the following command:

$ echo IdKey id\_rsa\_2048\_<hostname> > identification

4. Add public key to authorized\_keys file on remote server

Run the following command to append your public key to the *authorized\_keys* file on the remote server:

$ cat id\_rsa\_2048\_<hostname>.pub.ssh| ssh <your login>@<hostname> "mkdir .ssh && cat >> ~/.ssh/authorized\_keys"

Or, if you already have a .ssh directory inside your $HOME:

$ cat id\_rsa\_2048\_<hostname>.pub.ssh| ssh <your login>@<hostname> "cat >> ~/.ssh/authorized\_keys"

Repeat this command to update the *authorized\_keys* file for every server you want to be able SSH to.

5. If ssh to remote host via authorized\_keys fails,

From ~/ on the remote server:

$ restorecon -FRv ~/.ssh

Repeat this command on all servers with broken ssh authorized keys connection.