This guide describes how to generate and use a private/public key pair to log in to a remote system with SSH using [PuTTY](http://www.chiark.greenend.org.uk/%7Esgtatham/putty/download.html). PuTTY is an SSH client that is available for Windows and Linux (although it is more common on Windows systems). Using key-based SSH logins, you can disable the normal username/password login procedure which means that only people with a valid private/public key pair can log in. That way, there is no way for brute-force attacks to be successful, so your system is more secure.

**1 Preliminary Note**

In this tutorial I use a Windows desktop to connect to a Linux SSH server (Debian with IP address: 192.168.0.100).

**2 Install PuTTY, PuTTYgen, And Pageant On The Windows System**

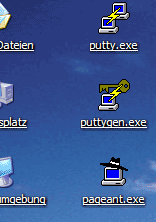
First we need to install PuTTY, PuTTYgen, and Pageant on our Windows system. All we need to do is download the exectuable files (.exe) and save them somewhere, e.g. on the desktop. We don't need to install them as they are standalone applications. To start them, we only need to double-click them.

Download the following files from the [PuTTY download page](http://www.chiark.greenend.org.uk/%7Esgtatham/putty/download.html) and save them on your Windows system, e.g. on the desktop:

[http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe](http://the.earth.li/%7Esgtatham/putty/latest/x86/putty.exe)

[http://the.earth.li/~sgtatham/putty/latest/x86/puttygen.exe](http://the.earth.li/%7Esgtatham/putty/latest/x86/puttygen.exe)

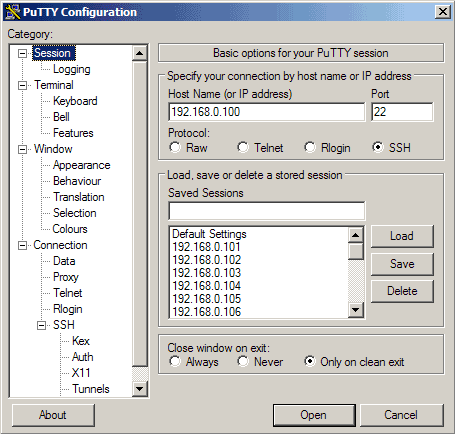
[http://the.earth.li/~sgtatham/putty/latest/x86/pageant.exe](http://the.earth.li/%7Esgtatham/putty/latest/x86/pageant.exe)

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/1.png)

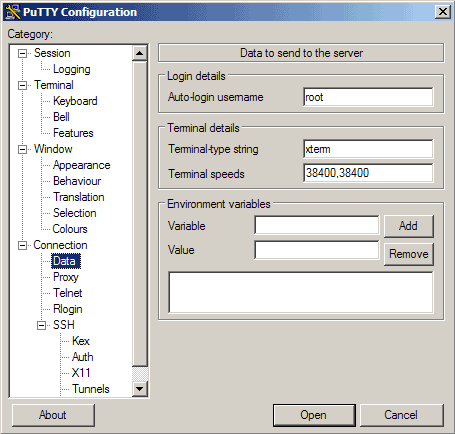
**3 Create A Profile With Settings For Our 192.168.0.100 Server**

In PuTTY, you can create profiles for connections to your various SSH servers, so you don't have to type in the settings again when you want to connect to a certain server again.

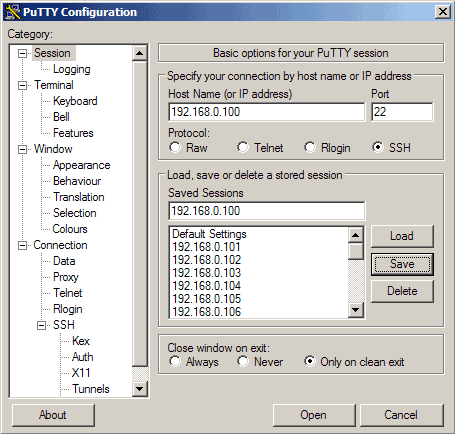
Let's create a profile for our 192.168.0.100 server. Start PuTTY by double-clicking its executable file. You are now in the category Session (see the tree on the left side of the screenshot). Enter 192.168.0.100 under Host Name (or IP address), enter 22 under Port and select SSH under Protocol:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/2.png)

Then go to Connection -> Data and specify the username with that you want to log in to your SSH server under Auto-login username. In this article I use root:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/3.png)

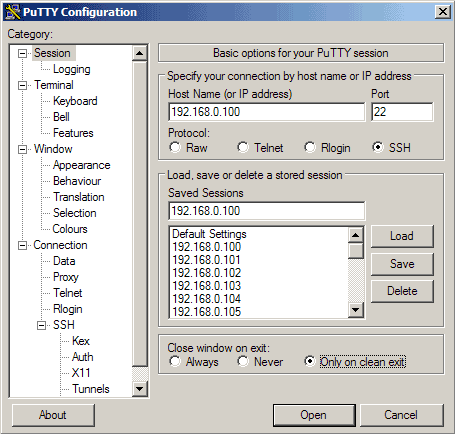
Then go to Session again. Under Saved Sessions enter a name for the profile, e.g. 192.168.0.100 or any other string that lets you remember for which server the profile is. Then click on Save:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/4.png)

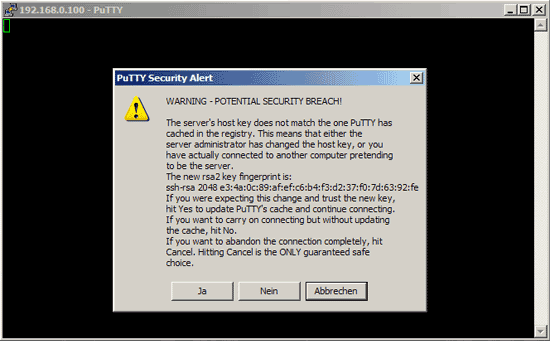
The next time you use PuTTY, you can simply select the appropriate profile from the Saved Sessions textarea, click on Load and then Open.

**4 Connect To The SSH Server**

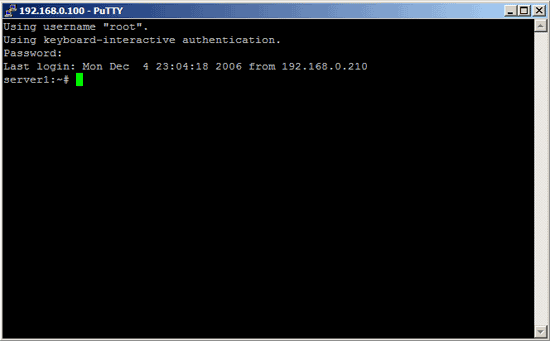
Now we can connect to our SSH server simply by clicking on Open.

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/5.png)

If you connect to the server for the first time, a security warning pops up. This is because PuTTY doesn't know the server's host key yet, so it is safe to click on Yes. (If this happens again later on, this can mean that another server is now running under the same IP address, or that someone has broken in and changed the key.)

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/6.png)

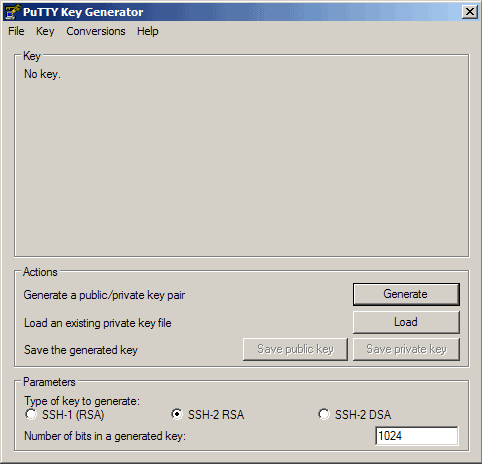
We have saved the username with which we connect in our profile settings, so we don't have to type it here again. We only have to specify that user's password:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/7.png)

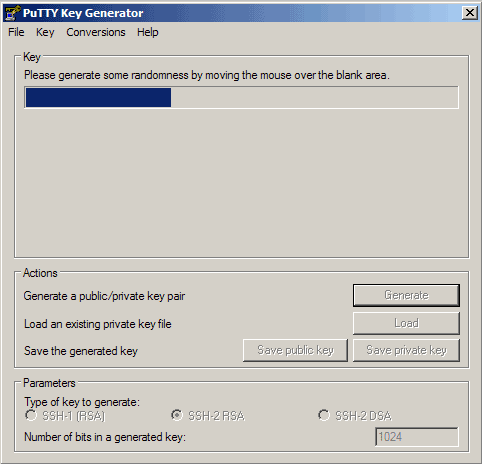
Now this was the "normal" way of logging in, i.e., with a username and a password. If anyone else knows the username and password, he can log in, too. So if you have weak passwords and/or are the victim of a brute-fore attack, this can become a problem. Let's change that now.

**5 Generate A Private/Public Key Pair**

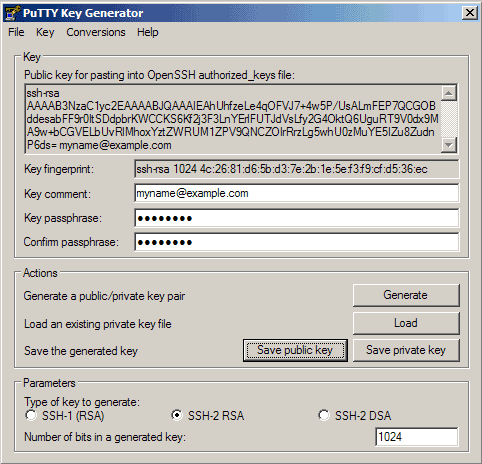
We can use PuTTYgen to create a private/public key pair. Start it by double-clicking its executable file. Make sure you select SSH-2 RSA under Type of key to generate and specify 1024 as the Number of bits in a generated key. Then click on Generate:

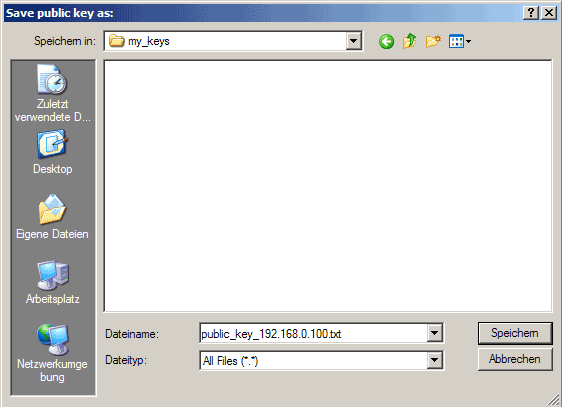
[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/8.png)

Please move the mouse pointer over the blank area during the key generation to generate some randomness:

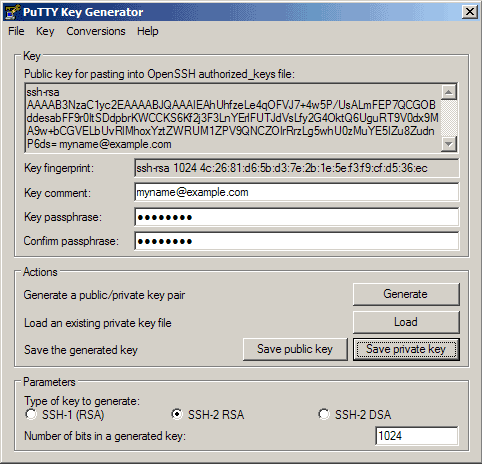
[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/9.png)

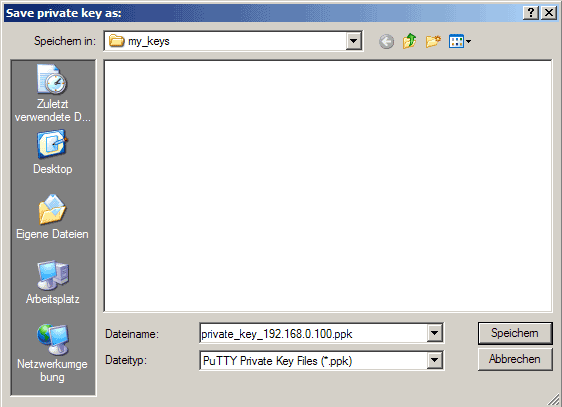
Now a private/public key pair has been generated. Under Key comment, you can enter any comment; normally you use your email address here. Then specify a Key passphrase and repeat it under Confirm passphrase. You'll need that passphrase to log in to SSH with your new key. Then click on Save publick key and save it in some safe location on your computer. You are free to choose a filename and extension, but it should be one that lets you remember for which system it is.

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/10.png)

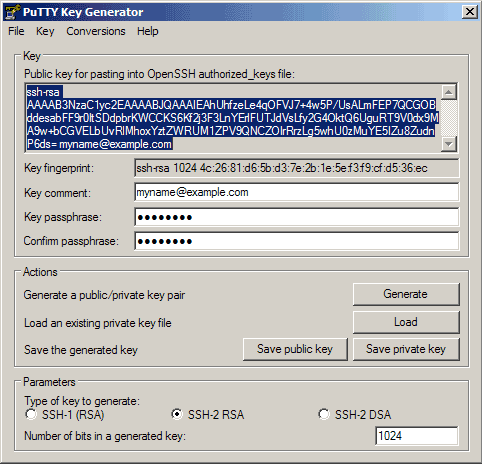
[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/11.png)

Then click on Save private key. You can save it in the same location as the public key - it should be a location that only you can access and that you don't lose! (If you lose the keys and have disabled username/password logins, then you can't log in anymore!) Again, you're free to choose a filename, but this time the extension must be .ppk:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/12.png)

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/13.png)

Then copy the public key from the PuTTYgen window:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/14.png)

**6 Save The Public Key On The Server**

Then log in to your SSH server (if you have closed the previous SSH session already), still with the username and password, and paste the public key into the file ~/.ssh/authorized\_keys2 (in one line!) like this:

mkdir ~/.ssh  
chmod 700 ~/.ssh

vi ~/.ssh/authorized\_keys2

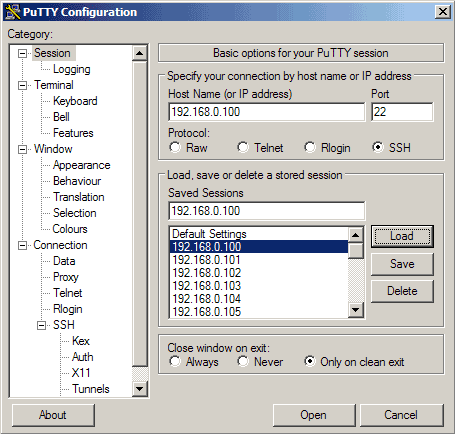
ssh-rsa AAAAB3NzaC1yc2EA[...]Lg5whU0zMuYE5IZu8ZudnP6ds= myname@example.com

That file must be write/readable only by that user, so we run

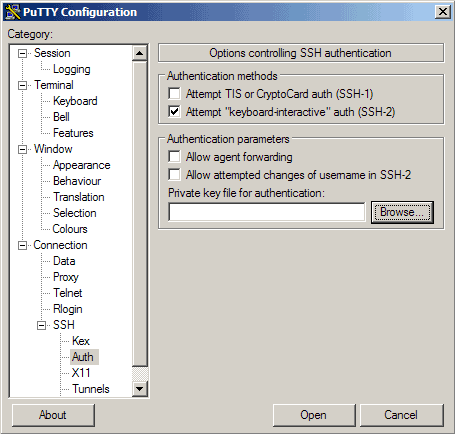
chmod 600 ~/.ssh/authorized\_keys2

## 7 Attach The Private Key To The PuTTY Profile

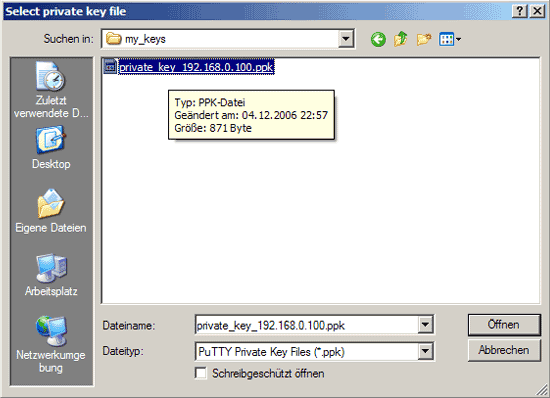
Now launch PuTTY again and load the profile of your SSH server (192.168.0.100):

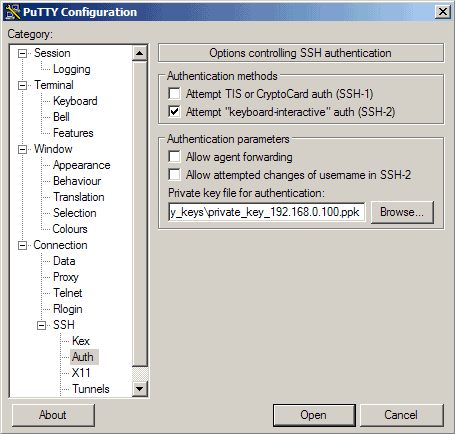
[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/15.png)

Then go to SSH -> Auth and click on Browse:

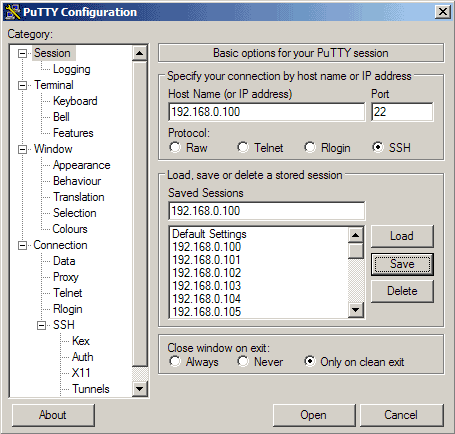
[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/16.png)

Browse your file system and select your previously created private key:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/17.png)

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/18.png)

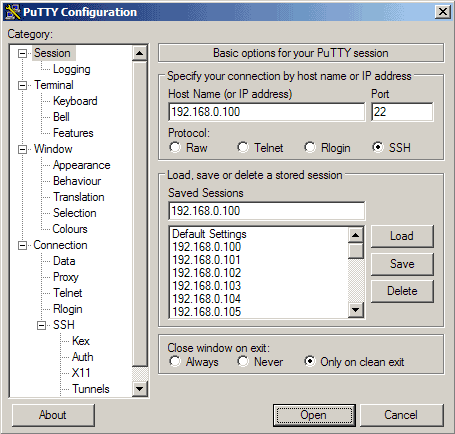
Then go to Session again and click on Save:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/19.png)

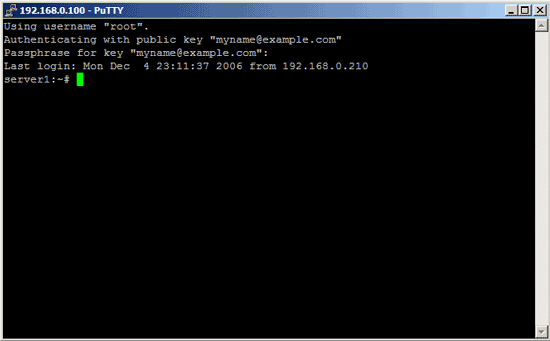
Now we have attached the private key to our 192.168.0.100 PuTTY profile.

## 8 Our First Key-Based Login

Now everything is ready for our first key-based login to our SSH server. Click on Open:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/20.png)

As you can see, the public key is now used for authentication, and you are asked for the passphrase (the one you specified in chapter 5):

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/21.png)

## 9 Disable Username/Password Logins

Up to now, you can log in with your private/public key pair and still with username/password logins, so if someone doesn't attach a private key to his PuTTY session, he will be asked for a username and password. So to achieve a better security, we must disable the username/password logins (you should do this only when you know that your key-based logins are working, because if they aren't and you disable username/password logins, then you have a problem...).

To disable the username/password logins, we must modify the sshd configuration file. On Debian/Ubuntu systems, it's /etc/ssh/sshd\_config. You should set Protocol to 2 (1 is insecure and should not be used!), PasswordAuthentication to no, and UsePAM to no (or comment out the UsePAM line), e.g. like this:

vi /etc/ssh/sshd\_config

[...]

Protocol 2

PasswordAuthentication no

UsePAM no

[...]

Then restart sshd. On Debian/Ubuntu, you can do it like this:

service ssh restart

On Older versions, use the init script instead of the service command:

/etc/init.d ssh restart

Now if you open a PuTTY session without your private key attached, you shouldn't be able to log in anymore.

## 10 Let Pageant Remember Your Key Passphrase

Whenever you use your key-based login now, you stilll have to specify your key passphrase. This can be annoying if you connect to the SSH server multiple times a day. Fortunately, you can tell the passphrase to Pageant which will then provide the passphrase whenever you log in to your SSH server.

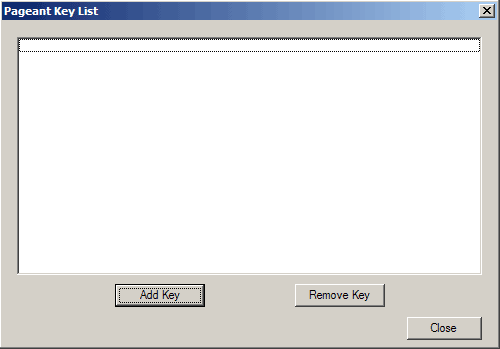
You can start Pageant by double-clicking its executable file:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/22.png)

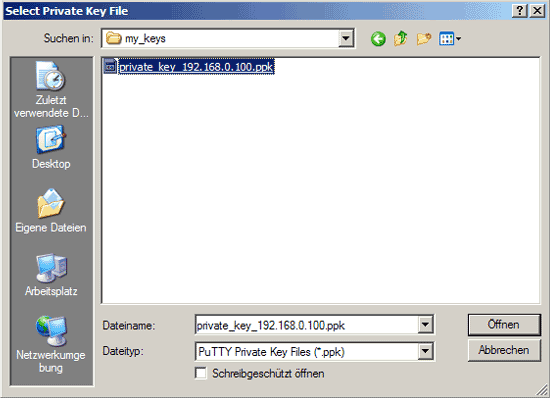
Afterwards, you should see running Pageant in the taskbar:

[https://www.howtoforge.com/images/ssh_key_based_logins_putty/23.png](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/23.png)

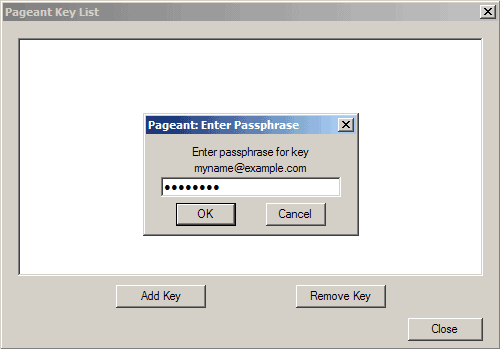
Now double-click the Pageant icon in the taskbar. The following window comes up. Click on Add Key:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/24.png)

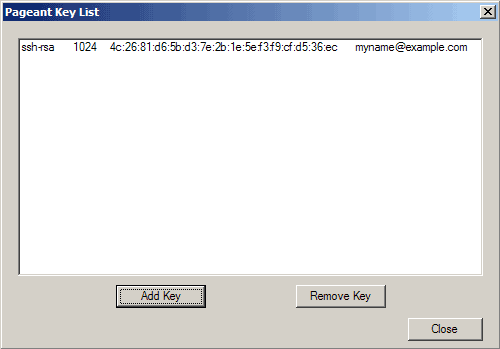
Browse your filesystem and select your private key:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/25.png)

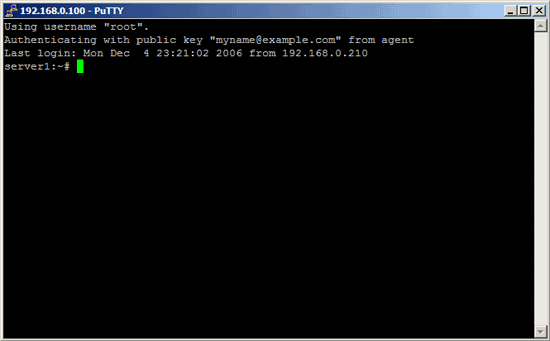
Then enter the passphrase for the private key:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/26.png)

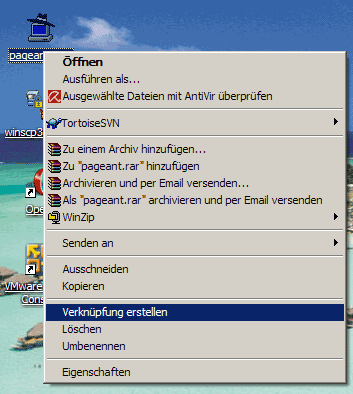
The key is now listed in Pageant's key list. Click on Close:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/27.png)

As long as Pageant is running in the taskbar, you can log in to your SSH server without providing the passphrase - this is done by Pageant:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/28.png)

When you stop Pageant, it forgets all keys, so the next time you start Pageant you must add the keys again. This can also be annoying, but to prevent this, we can create a shortcut on the desktop to the Pageant executable. Right-click the Pageant executable and select Create Shortcut:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/29.png)

You should now find a shortcut. Right-click it and go to Properties:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/30.png)

Under Target, you will now find the path to pageant.exe, e.g. "C:\Dokumente und Einstellungen\falko\Desktop\pageant.exe" (if there are no spaces in your path, you don't need the quotation marks). You can now simply add the location of your private key to that line, for example if you private key is C:\putty\my\_keys\private\_key\_192.168.0.100.ppk then the line should look like this:

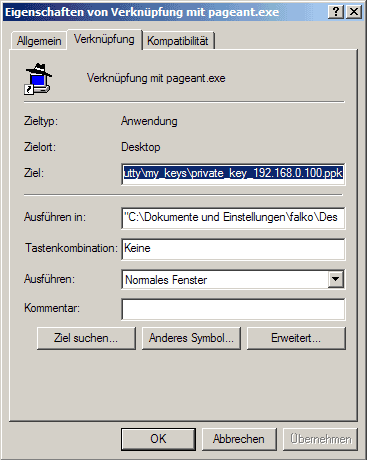
"C:\Dokumente und Einstellungen\falko\Desktop\pageant.exe" C:\putty\my\_keys\private\_key\_192.168.0.100.ppk

(if there are spaces in the path to your private key, you must wrap it in quotation marks again, e.g. like this:

"C:\Dokumente und Einstellungen\falko\Desktop\pageant.exe" "C:\directory with lots of spaces in name\my keys\private\_key\_192.168.0.100.ppk"

)

Then click on OK:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/31.png)

Now when you double-click on the Pageant shortcut, Pageant will automatically load your private key and ask you for the passphrase. Enter it, and that's