

Secure Shell on Windows Using PuTTY

PuTTY is a free set of Windows tools that can be used to perform SSH tasks on Windows. This note shows how to use PuTTY to create a public/private key pair and then use it for SSH authentication.

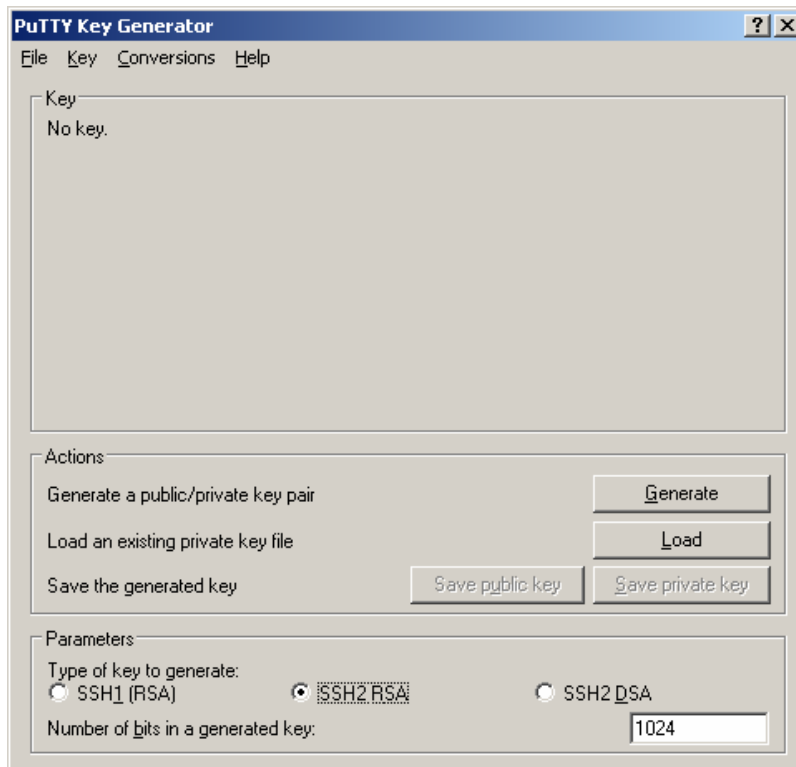
1. Obtaining PuTTY

For home use, it can be downloaded from: <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>. The windows installer is the most convenient one to use. PuTTY is actually a suite of several small, but extremely useful applications. The ones you will use are puttygen.exe, putty.exe, and pageant.exe.

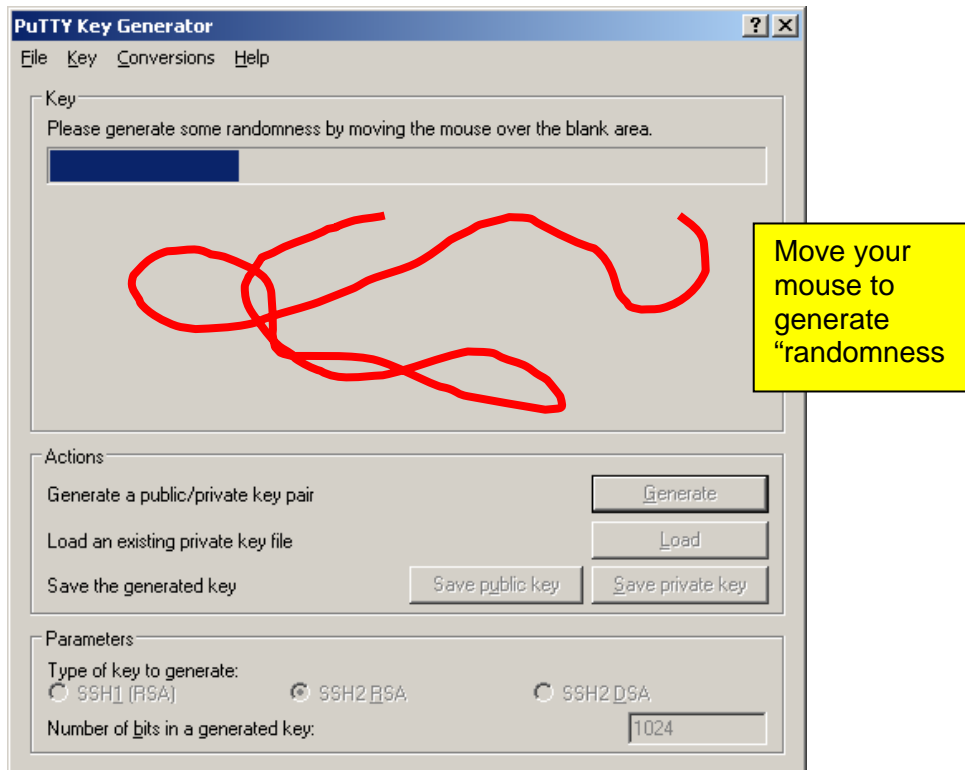
In the computer lab, all the necessary executable files are located on R:\PuTTY0.55.

2. Generating a Private Key

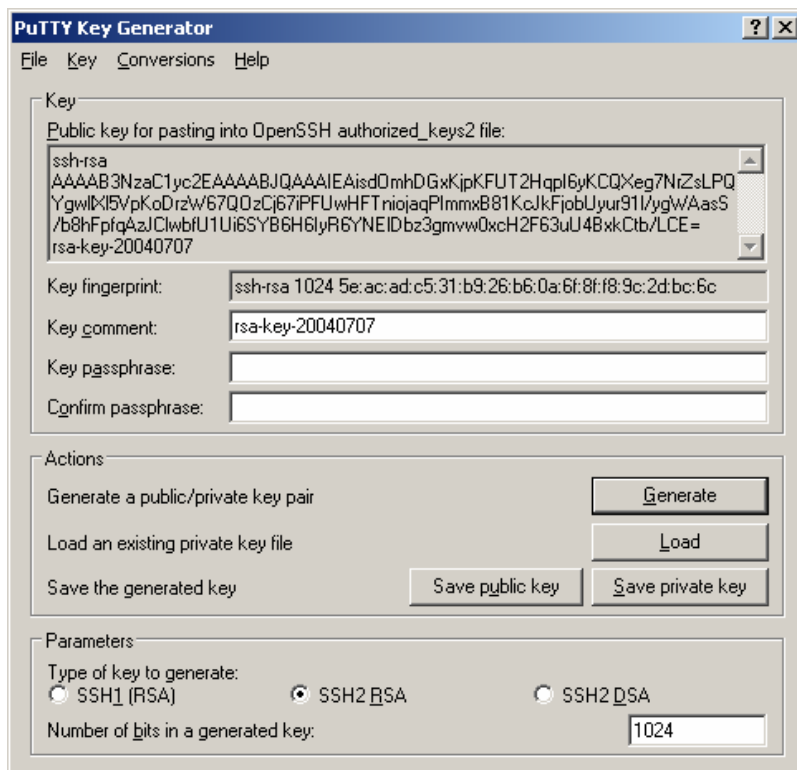
To connect to the CVS server securely, you need a public/private key pair. The public key will be installed on the server, and in general can be seen by anyone. and the private key should be kept secure and protected by a good passphrase. To create a public/private key, start the puttygen.exe application. It is located in R:\PuTTY in the lab, and in C:\Program Files\PuTTY (or wherever you installed it) if installed separately. After opening, click the “SSH2 RSA” radio button near the bottom of the window:



Next, click the Generate button and start moving the mouse at random in the blank area called “Key”:

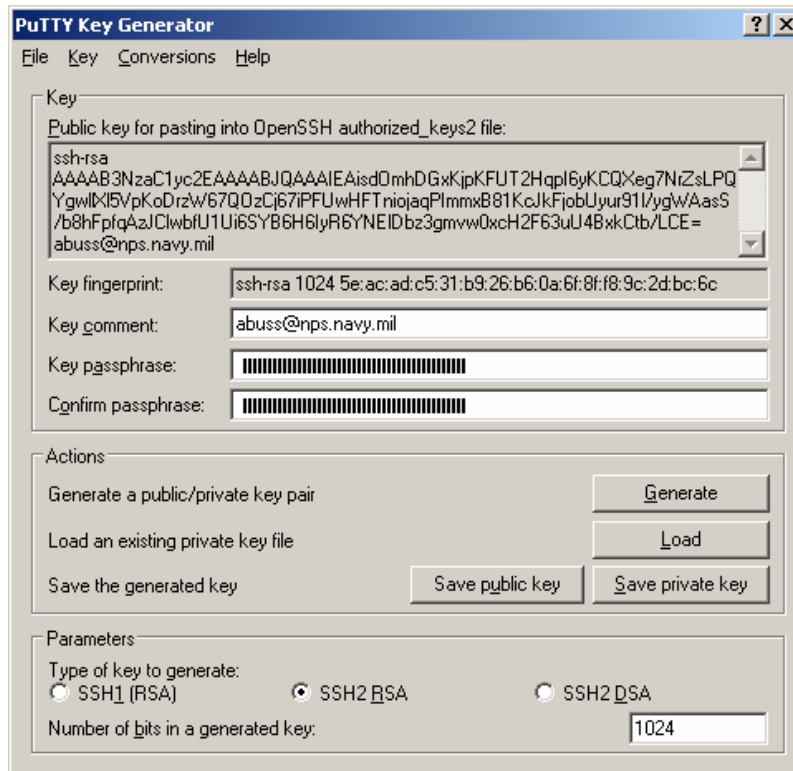


When enough “randomness” has been generated, puttygen will create the keys:

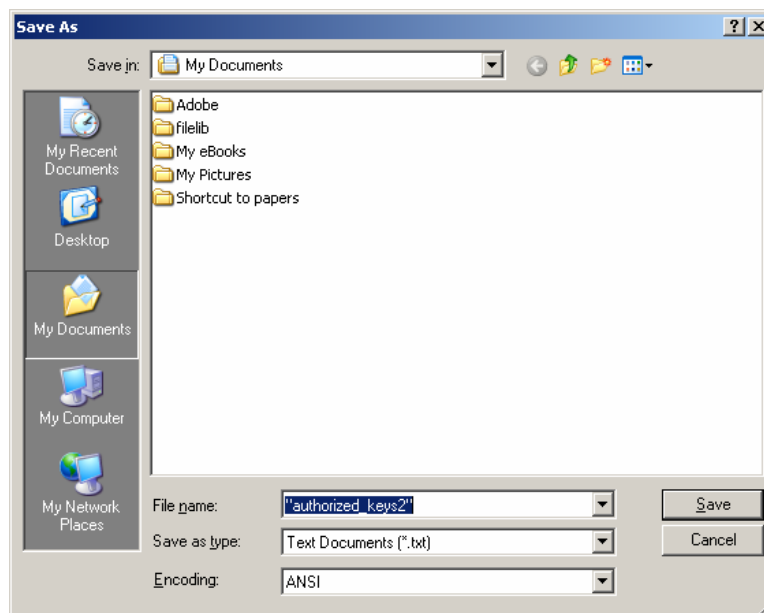


Change the Key Comment to your e-mail address and enter (twice) a reasonable

passphrase (ideally more than one word with spaces and non-alphanumeric characters).

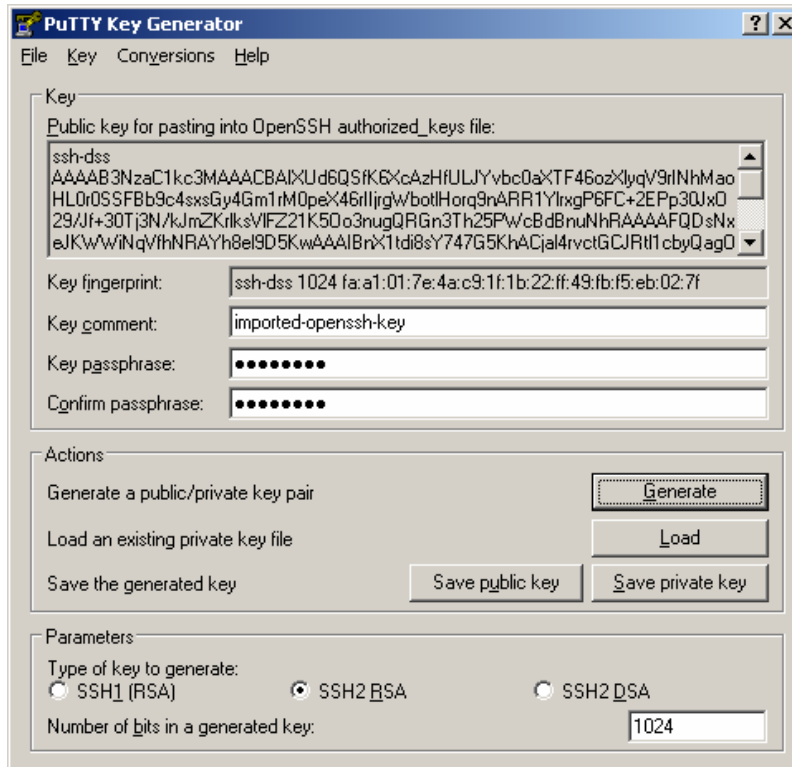


Click “Save private key” and save the file somewhere safe. One of the best options is to save it to a USB memory key. Do not close the puttygen window yet. Right-click in the area below “Public key for pasting into OpenSSH authorized_keys2 file:” and choose “Select All.” Right-click again in the highlighted area and choose “Copy.” Finally, open a plain text editor (Notepad), do a paste, and save it as a file called “authorized_keys2” – note, be sure to put double-quotes around “authorized_keys2” or notepad will append “.txt”:



3. Importing an Existing Key

If you already have an SSH public/private key pair you wish to use, you will need to import it into PuTTY's format to use it in the manner described in this note. Open Conversions | Import Key and select your private key file. You will be prompted for your passphrase and, if correctly entered, will load your key into PuTTYGen:



Change the Key Comment to your e-mail address and proceed as above. You can leave your passphrase the same as for your existing key or enter a new one.

4. Installing Public Key on the Server

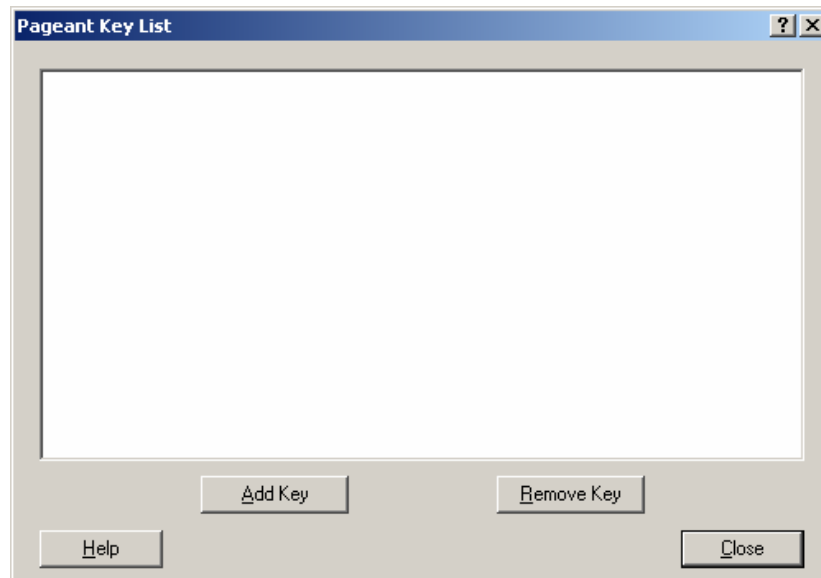
The administrator of the CVS server will create an account for you and will need a copy of your public key (the authorized_keys2 file you generated above). This account needs to be setup before proceeding. Also, for security purposes, the administrator will most likely require you to give the public key in person.

5. Saving a Session in PuTTY

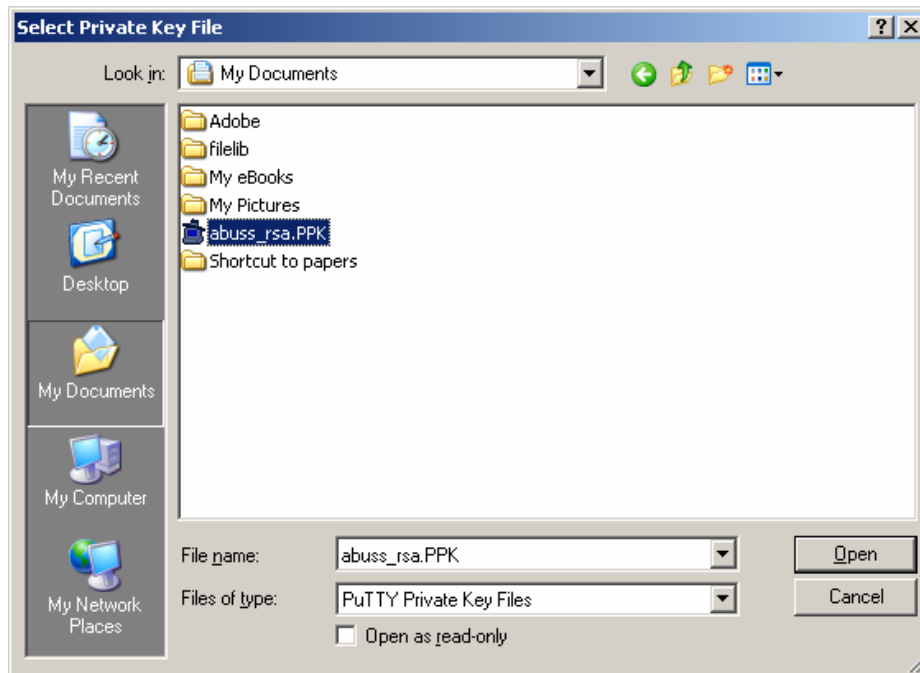
Now that you have an account on the CVS server, there are still a few more steps that must be taken to configure your windows machine. First, run the pageant program. If you have installed PuTTY you can run it from Start | Programs | PuTTY; or you can open R:\PuTTY and double-click pageant.exe. After waiting for something to happen, you will remember that the only thing is that the pageant icon appears in the system tray:



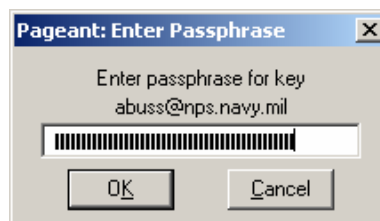
Double-clicking on the pageant icon will bring up the key selection window:



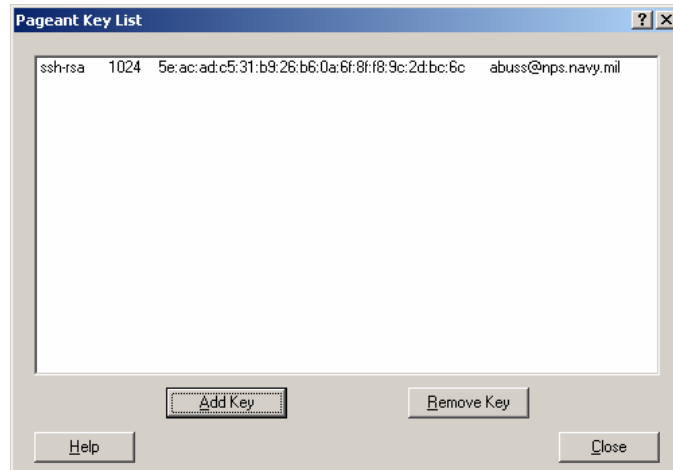
Click "Add Key" and navigate to your private key file:



After opening, you will be asked for your private key passphrase:

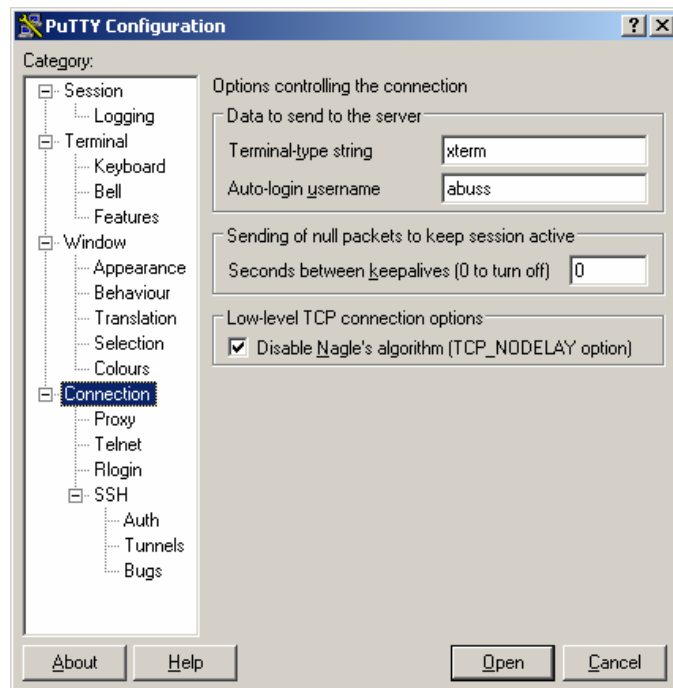


If successful, you will see your private key has been added:

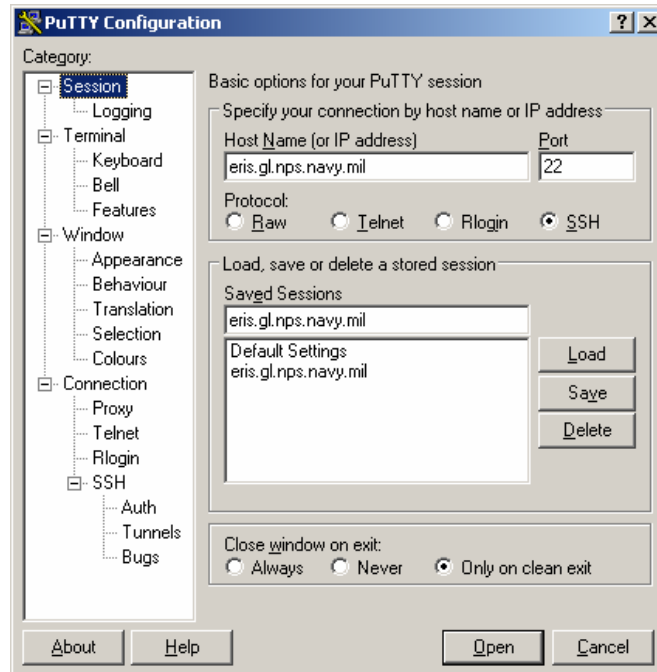


Note: Each login session you will have to repeat this step with pageant if you are going to be using CVS.

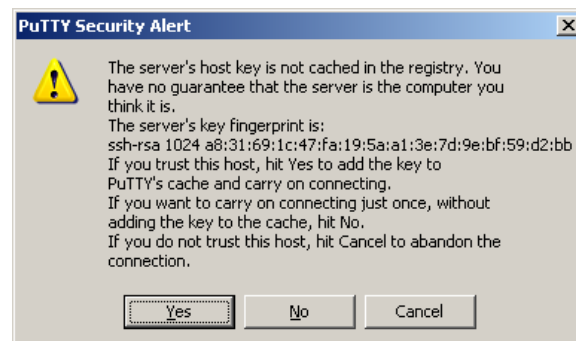
Once you have successfully added your private key, close this window and start PuTTY. Since you will always be using SSH 2, first click on the radio button labeled “SSH” under “Protocol: Then click SSH in the tree on the left and click “2” under “Preferred SSH protocol version:” Select Connection on the left and enter your user name (on the CVS server):



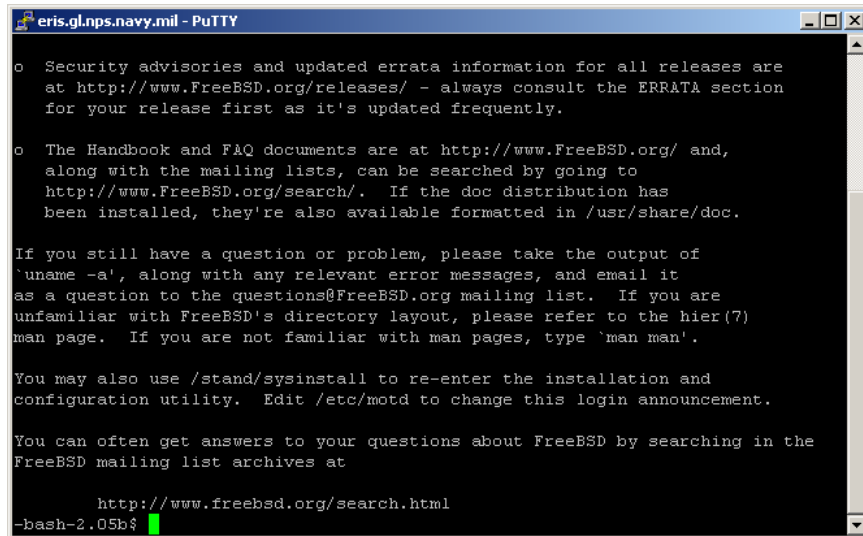
Click “Session” and enter the server’s IP address as both the “Host Name” and the “Saved Sessions”. Click Save:



You can actually name the session anything you want. However, that saved name is used by Netbeans to connect to the server (not the server's "real" address). You must have a saved session in putty for Netbeans to work with it. If you now click "Open" you should get the following message:



Check to be sure that the server's key fingerprint is identical to the characters following "ssh-rsa 1024". They most likely will be, unless someone is spoofing the CVS server. Assuming this checks out, click "Yes." The server's key must be cached in the registry for PuTTY to be able to work with Netbeans. If all goes well, you should be logged on to the CVS server without having to type in a password to it:



```
eris.glnps.navy.mil - PuTTY

o Security advisories and updated errata information for all releases are
  at http://www.FreeBSD.org/releases/ - always consult the ERRATA section
  for your release first as it's updated frequently.

o The Handbook and FAQ documents are at http://www.FreeBSD.org/ and,
  along with the mailing lists, can be searched by going to
  http://www.FreeBSD.org/search/. If the doc distribution has
  been installed, they're also available formatted in /usr/share/doc.

If you still have a question or problem, please take the output of
'uname -a', along with any relevant error messages, and email it
as a question to the questions@FreeBSD.org mailing list. If you are
unfamiliar with FreeBSD's directory layout, please refer to the hier\(7\)
man page. If you are not familiar with man pages, type 'man man'.

You may also use /stand/sysinstall to re-enter the installation and
configuration utility. Edit /etc/motd to change this login announcement.

You can often get answers to your questions about FreeBSD by searching in the
FreeBSD mailing list archives at

http://www.freebsd.org/search.html

-bash-2.05b$
```

Once this works you should immediately logout (enter “logout”) if you are to be using this primarily for CVS over SSH. Once the host key has been cached on a windows machine you should never log in through a terminal again from that machine. Once the host key is cached, it will stay that way (an entry is created in your Windows registry that persists). If you are logged in to your NPGS account, the key will be written to your Windows profile, so on campus you will only have to cache the host key once, period.

For CVS over SSH, this is all that is needed. If you will be using PuTTY to actually log into the remote machine, then load your private key into Pageant and then run PuTTY as shown above. Once logged in, your terminal should be approximately whatever the shell is on your remote machine; “approximately,” since not all shell functionality is emulated by PuTTY.