Contents

[SSH Key Creation and Usage 1](#_Toc361645484)

[Creating an SSH Key Using Windows 1](#_Toc361645485)

[Export Putty Private Key to OppenSSH Format 6](#_Toc361645486)

[Configure Linux to use Multiple Private SSH Keys 7](#_Toc361645487)

[Creating an SSH Key in Ubuntu 12.04 7](#_Toc361645488)

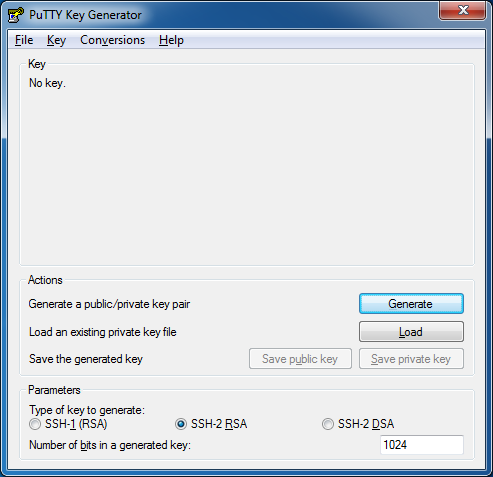
[Resources 8](#_Toc361645489)

# SSH Key Creation and Usage

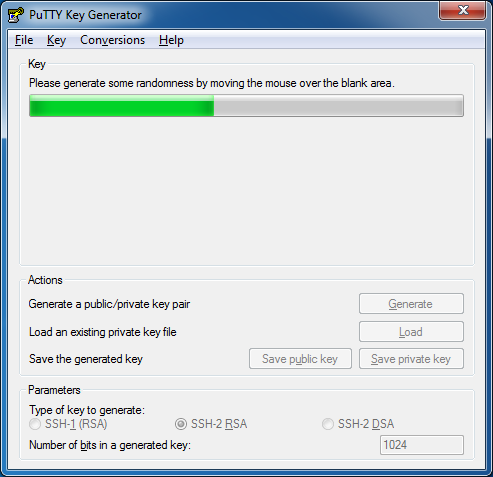
|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Create Key in | |
| Use Key in |  | Windows | Linux |
| Windows |  |  |
| Linux |  |  |

## Creating an SSH Key Using Windows

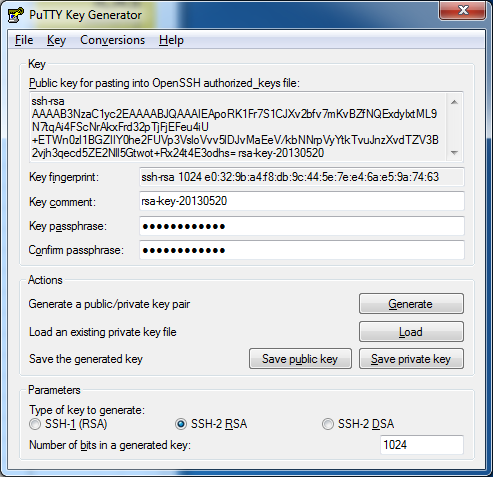
1. Download and run PuttyGen: <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>



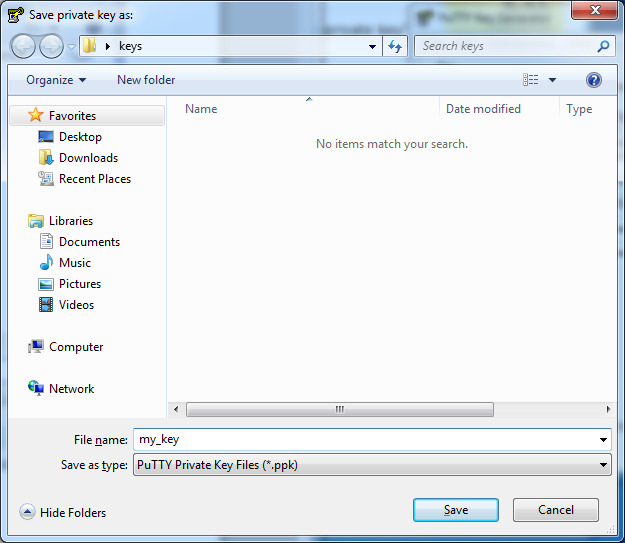
1. Click the “Generate” button and move the mouse around the “Putty Key Generator” window until the green bar is filled:



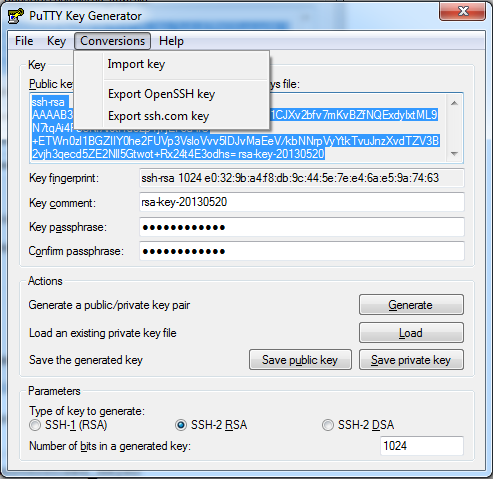
1. Set a strong “Key passphrase” to protect your SSH key being used by someone else (If you want to change the default “Key comment” then change it to something which identifies the user and computer on which the private key was generated and will be used):



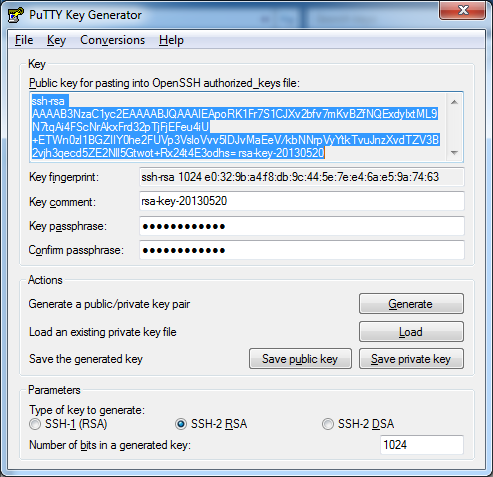
1. Click the “Save private key” button and type a filename (this will be used by Putty in SSH connections):



* 1. This private key will be used by Putty whenever you try to connect to another server via SSH.



1. Copy the ssh-rsa public key text to the clipboard for use on your Linux server(s):



* 1. Save this on the Linux server you would like to SSH into:

mkdir ~/.ssh && chmod 700 ~/.ssh

nano ~/.ssh/authorized\_keys2

ssh-rsa AAAAB3NzaC1[…]3qot+Rx24t4E3odhs= rsa-key-20130520

chmod 600 ~/.ssh/authorized\_keys2

* 1. The server may provide a web interface for adding this public key e.g. github, code.acpfg.local, …
  2. At this point you should now be able to connect to the server using Putty.

### Export Putty Private Key to OppenSSH Format

It is usually not good practice to use the same private key from multiple computers. However, there are times when online services will create a single private key for you to subsequently use with that service. E.g. the NeCTAR Research Cloud. This often means you want to distribute this private key to multiple machines from which you will use that service. You can convert the Putty private key into an openSSH format as follws:

1. Load the Putty private key
2. Click the “Conversions” menu and choose “Export OpenSSH key” and choose a filename.

### Configure Linux to use Multiple Private SSH Keys

1. Copy the OpenSSH private key file to a Linux server. For consistency, use a filename like: ~/.ssh/id\_rsa.<some\_string>
2. Make the file only readable/writable by yourself:

chmod 600 ~/.ssh/id\_rsa.<some\_string>

1. Configure SSH to attempt to also use this alternative private key during SSH authentication. Simply append the following line to the ~/.ssh/config file:

IdentityFile ~/.ssh/id\_rsa.<some\_string>

## Creating an SSH Key in Ubuntu 12.04

1. Create a private/public key pair:

ssh-keygen -t rsa

ssh-add ~/.ssh/id\_rsa**Copy Public Key to a Server**

1. Copy the public ID to the machine you wish to connect to:

ssh-copy-id user@server

# Resources

<http://www.howtoforge.com/ssh_key_based_logins_putty>