**Using-ssh-with-rsa-keys**

**Setting up SSH public/private keys**

**SSH Version 2**

To pass the shared key to other servers you must run the following commands, replacing username for the user you are updating.

Either log in as root and run

|  |
| --- |
| su – username |

Or just log in as the user and skip to the create the key step.

now create the key

|  |
| --- |
| ssh-keygen -t rsa -b 5120 |

now make sure the permissions are correct for the user

|  |
| --- |
| chmod 700 .ssh  chmod 600 .ssh/id\_rsa  chmod 644 .ssh/id\_rsa.pub  chmod 600 .ssh/id\_dsa  chmod 644 .ssh/id\_dsa.pub  chmod 644 .ssh/authorized\_keys |

Next you put the files on the server

|  |
| --- |
| cd ~/.ssh  sftp gituser@ipaddress  put id\_rsa.pub  exit |

Next you import the key on the remote server.

|  |
| --- |
| ssh gituser[@ipaddress](mailto:root@ipaddress)  cat id\_rsa.pub >> .ssh/authorized\_keys |

Finally you make sure the permissions are correct on the remote server

|  |
| --- |
| chmod 700 .ssh  chmod 600 .ssh/id\_rsa  chmod 644 .ssh/id\_rsa.pub  chmod 600 .ssh/id\_dsa  chmod 644 .ssh/id\_dsa.pub  chmod 644 .ssh/authorized\_keys  exit |