SSH Key Management

SSH Keys is a way of identifying yourself to an SSH server using cryptography instead of the traditional username and password combination. This method has several advantages over the password based authentication: the passwords are not sent to trough the network, there is no risk for brute force attacks and when using together with the SSH agent it is possible to login to multiple servers without entering your credentials again and again.

At IFCA it is highly reccomended to use SSH Key authentication for accessing the Cluster.

We reccomend the reading of the fantastic Arch Linux SSH Keys guide for more details. Some instructions are provided below though.

SSH Key creation

Windows (PuTTY)

Check this page for more information.

Linux

Check this page for more information.

Upload key

Once you have your key ready, you must install it on the server you are going to access.

Using the authorized_keys file

You have to access (using SSH and your username and password) to the machine where you want to use your public key and add the contents of your public key file to the .ssh/authorized_keys. If you are using GNU/Linux, you can add it with the following command:

```
$ ssh-copy-id username@gridui.ifca.es
```

This will install your ssh public key at Scientific Linux 6 infrastruccture.