Create a ssh key

Access to the CNCA computing clusters is performed via SSH and requires the use of SSH keys for authentication. Authentication with passwords is not supported. Each SSH key pair has two components a **public key** that must be added to the hosts to be remotely accessed, and a **private key** that must remain in the user workstation or laptop machine. The private key must be protected with a **strong password**. The users must generate their own SSH key pair in a machine of their own (workstation, laptop, etc). To generate your SSH key pair follow these instructions.

Linux and macOS

- Users must generate the SSH key pair in a computer of their own (desktop, notebook etc).
- The passphrase is used to protect the private key, very IMPORTANT please choose a strong password with uppercase and lowercase characters, numbers and symbols.

NOTE: xxx will be rsa, ed25519 or something similar. And you must check and replace it accordling in the instructions below.

```
$ ssh-keygen -b 4096
Generating public/private xxx key pair.
Enter file in which to save the key (/home/username/.ssh/id_xxx):
Created directory '/home/username/.ssh'.
Enter passphrase (empty for no passphrase):           ----> IMPORTANT: Choose a strong
password
Enter same passphrase again:                          ----> IMPORTANT: Choose a strong
password
Your identification has been saved in /home/username/.ssh/id_xxx
Your public key has been saved in /home/username/.ssh/id_xxx.pub
```

- ssh-keygen will create a pair of keys, private (id_xxx) and public (id_xxx.pub), these files are created in the user home directory usually under $HOME/.ssh
- The file and directory protections of $HOME/.ssh should be as follows:

```
ls -la $HOME/.ssh/
total 8
drwx------ 3 username group 4096 Jan 11 18:12 .
-rw------- 1 username group 1743 Feb 19 10:52 id_xxx
```

```
-rw-r--r-- 1 username group  404 Feb 19 10:52 id_xxx.pub
```

- Correct File permissions using chmod

```
chmod 700 .ssh
chmod 644 id_xxx.pub
chmod 600 id_xxx
```

- Users must send to the CNCA administrators **only** the public key **id_xxx.pub** (full content of the file).
- The private key must must be kept private and must NEVER be shared with other persons.

Microsoft Windows

- For Windows users accessing the CNCA public machines we recommend the use of **terminal emulators** like **MobaXterm**.
  - MobaXterm works both as a terminal and X windows server, this allows to display in your desktop the graphical X11 windows from the remote Linux host.
  - MobaXterm supports file transfer via the embbed SFTP browser.
  - MobaXterm documentation is available **here**
  - Key pairs can be generated with `ssh-keygen -b 4096`
  - You can also create and manage your SSH keys using the embedded **MobaKeyGen** application (available from the "Tools" menu).

- Windows users can also generate ssh-keys using **Putty**
  - Download and install Putty
  - Generate the key in your Windows machine see these examples:
    - Youtube
    - HowTo
  - IMPORTANT: notice that Putty is only a text terminal and does not work as X windows graphics server and does not support file transfer.

- Users must send to the CNCA administrators **only** the public key **id_rsa.pub**
- The private key must must be kept private and must NEVER be shared with other persons.

Login does not work

- If the CNCA helpdesk confirms that your public key has been installed and still you cannot login please check the following:
  1. That you are trying to access the correct CNCA login hostname as indicated by the CNCA helpdesk.
  2. That you are trying to access the CNCA host from the same machine and user account where you generated the SSH key pair.
  3. That the permissions and ownership of your SSH directory and contained files are correct. The relevant Linux directory and files are below, see if they match the protections described in the Linux section above:
     - $HOME/.ssh
     - $HOME/.ssh/id_rsa
     - $HOME/.ssh/id_rsa.pub
  4. That the SSH private key password is correct. In Linux you can do this by trying to load the private key into the SSH agent with the command: `ssh-add`
  5. That the CNCA login host is reachable from your machine. From Linux you can use the command `nmap -P0 -p22 hostname` the returned port STATE for the SERVICE *ssh* (PORT 22/TCP) must be **"open"**. If the hostname does not resolve or the STATE is different from **"open"** (e.g. filtered) you may have a network connectivity problem.
  6. If you are on Windows consider to install a Linux virtual machine and perform the SSH access from that Linux VM. Notice that in this case you need to place the keypair (id_rsa and id_rsa.pub) in the Linux virtual machine or generate a new key pair in Linux and send it to the CNCA administrators. To install Linux on windows you can use:
     - An hypervisor such as **VirtualBox**
     - The **Windows Subsystem for Linux (WSL)**
- If you still can't login please contact the CNCA helpdesk and provide details on the error and verification steps that you already performed.

Revision #60
Created 2019-02-20 17:48:20 UTC by João Pina
Updated 2026-07-10 14:52:40 UTC by Jorge Gomes