

# Login por SSH por intercambio de claves

ssh keys exchange

Quiero iniciar sesion desde 'maquina1' con el usuario 'usuario' en 'maquina2'. Resumen:

Maquina	Usuario
maquina1	usuario
maquina2	usuario

## Recomendada

1. (maquina1) Creamos las claves para el usuario 'usuario':

```
ssh-keygen -t rsa
```

Pulsamos 'enter' para cada pregunta

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/usuario/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/usuario/.ssh/id_rsa.
Your public key has been saved in /home/usuario/.ssh/id_rsa.pub.
The key fingerprint is:
3c:f1:f0:36:98:c0:f4:e3:b5:39:01:36:ae:b7:b7:04 usuario@test-5.dev.jj.com
The key's randomart image is:
+--[ RSA 1024]-----+
|      . +          |
|     o + o         |
|    o * o          |
|   = X +          |
|  . E 0           |
|   . = o          |
|    . o           |
|     o .          |
|      .           |
+-----+

```

Habremos generado el siguiente archivo:

```
/home/usuario/.ssh/id_rsa.pub
```

2. (maquina1) Copiamos el archivo generado en el paso anterior a 'maquina2':

```
ssh-copy-id usuario@maquina2
```

## A mano

1. (maquina1) Creamos las claves para el usuario 'usuario':

```
ssh-keygen -t rsa
```

Pulsamos 'enter' para cada pregunta

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/usuario/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/usuario/.ssh/id_rsa.
Your public key has been saved in /home/usuario/.ssh/id_rsa.pub.
The key fingerprint is:
3c:f1:f0:36:98:c0:f4:e3:b5:39:01:36:ae:b7:b7:04 usuario@test-5.dev.jj.com
The key's randomart image is:
+--[ RSA 1024]-----+
|      . +      |
|    o + o      |
|    o * o      |
|      = X +     |
|    . E 0      |
|    . = o      |
|    . o        |
|    o .        |
|    .          |
+-----+

```

Habremos generado el siguiente archivo:

```
/home/usuario/.ssh/id_rsa.pub
```

2. (maquina1) Copiamos el archivo generado en el paso anterior a 'maquina2':

```
scp /home/usuario/.ssh/id_rsa.pub test-6.dev:/tmp/
```

3. (maquina2) Creamos si no lo estan directorios y archivos necesarios. Finalmente incorporamos el archivo de claves a la lista de maquinas autorizadas:

```
[[ ! .ssh ]]; mkdir .ssh
[[ ! .ssh/authorized_keys ]]; touch .ssh/authorized_keys
chmod 600 .ssh/authorized_keys
cat /tmp/id_rsa.pub >> /home/usuario/.ssh/authorized_keys
```

4. (maquina1) Deberiamos ser capaces de iniciar una session SSH desde 'maquina1' con el usuario 'usuario' en 'maquina2':

ssh maquina2

From:

<http://wiki.legido.com/> - **Legido Wiki**

Permanent link:

[http://wiki.legido.com/doku.php?id=informatica:linux:ssh:login\\_intercambio\\_claves](http://wiki.legido.com/doku.php?id=informatica:linux:ssh:login_intercambio_claves)



Last update: **2015/04/13 20:19**