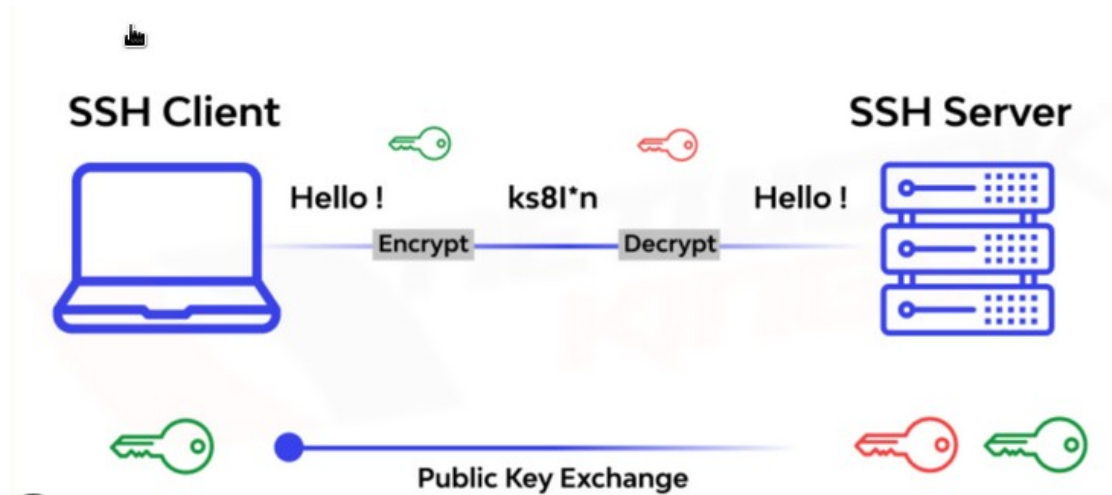


ssh

- SSH (**Secure Shell**) é un protocolo de rede que permite un acceso seguro a través de unha conexión cifrada.



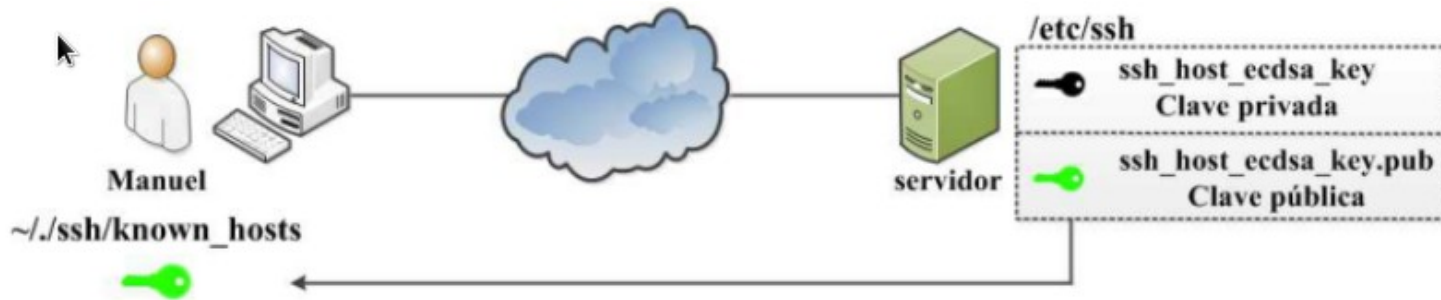
ssh- Servidor

Primeiro temos que **instalar** o Servidor ssh:

- sudo apt update
- sudo apt install openssh-server
- Arquivos ubicados en /etc/ssh:
 - **ssh-config**: aplicación cliente ssh
 - **sshd-config**: o **servidor** ssh
 - arquivos de clave pública – clave privada
- Podemos **xerar** de novo os arquivos de clave pública – privada con:
 - sudo **ssh-keygen -A**

ssh- Cliente

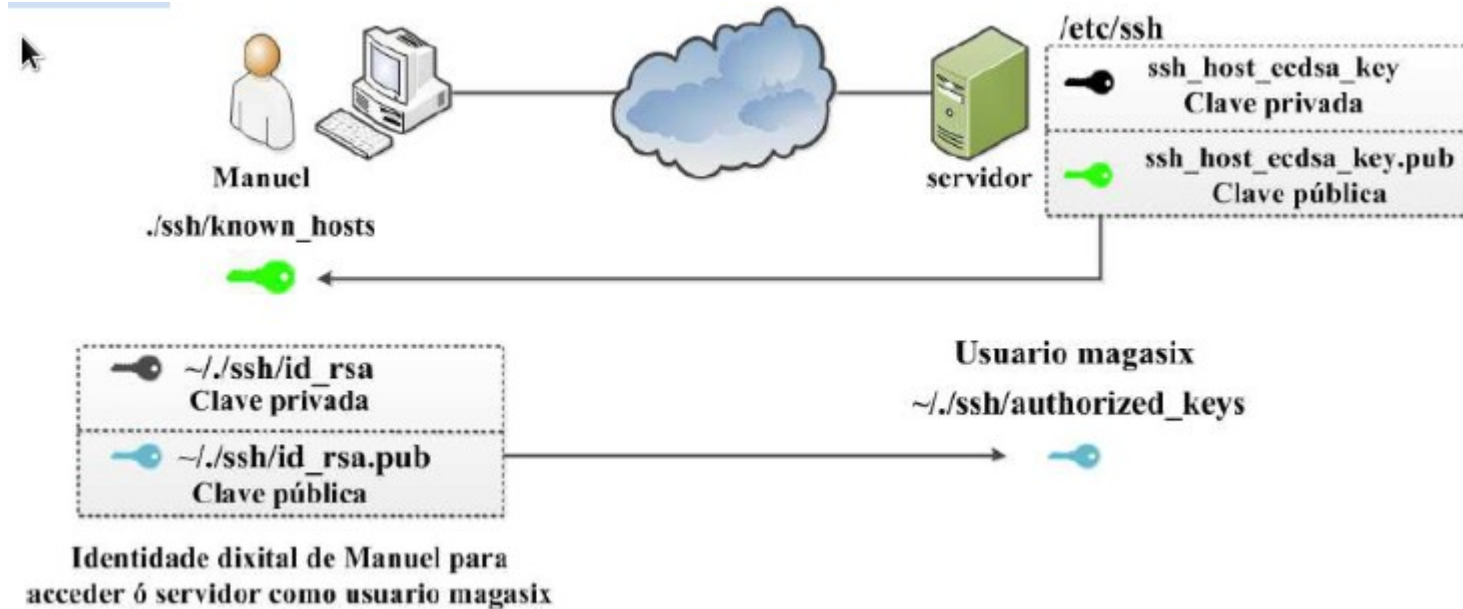
Cando o cliente se conecta por primeira vez, recibe a clave pública do servidor, coa que se encriptará a comunicación:



- A clave pública do equipo servidor gárdase no equipo cliente no **HOME** do usuario que inicia a conexión, na súa carpeta **.ssh** (oculta), no arquivo **known_hosts**

Autenticación por claves

SSH permite autenticar aos usuarios facendo uso de identidades dixital (formadas cunha parella de claves privada-pública) e os algoritmos criptográficos de clave simétrica. O procedemento a seguir é **crear a identidade dixital** e **copiar** a clave **pública** no arquivo de claves autorizadas no host remoto

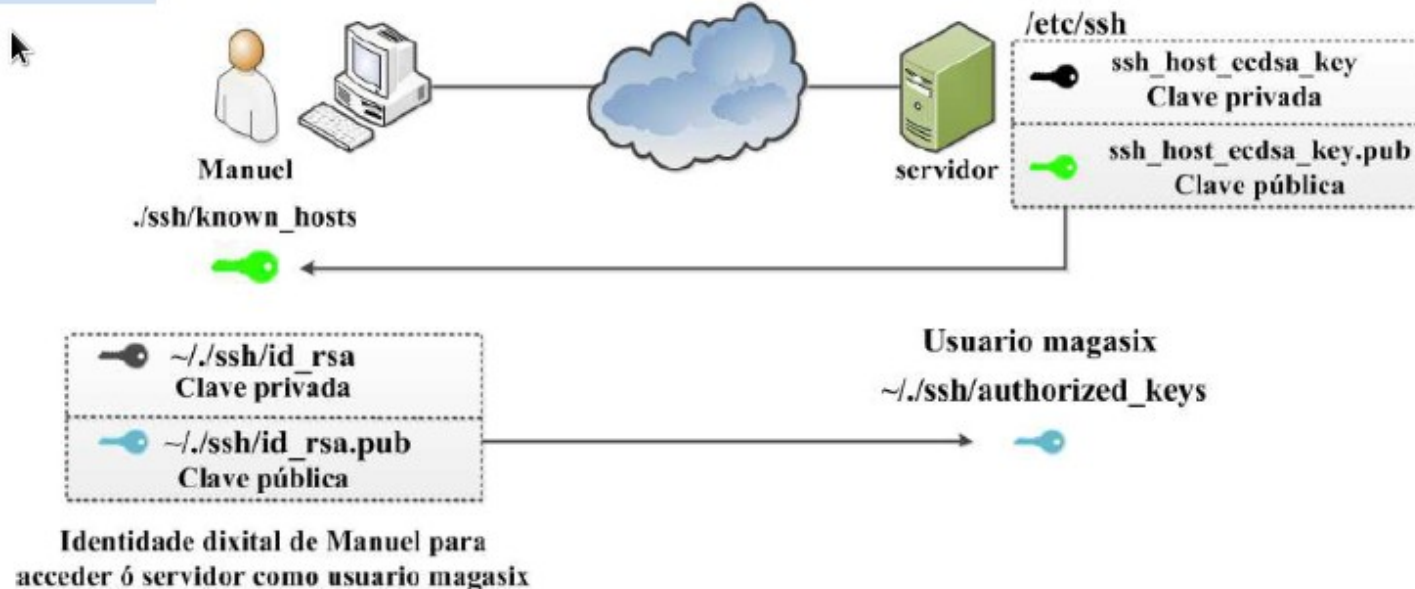


Autenticación por claves

O usuario do equipo cliente pódese conectar cun usuario con outro nome no servidor. Neste exemplo **Manuel** se conecta co usuario **magasix**.

¿¿Onde se gardan as claves??

- no cliente na carpeta **.ssh** do home de **manuel**
- no servidor na carpeta **.ssh** do home de **magasix**



Autenticación por claves

1. CREACIÓN de claves **no cliente**

Para la creación de claves empleamos el comando **keygen**:

```
$ ssh-keygen -f ~/.ssh/id_jefe_server1 -C "id para jefe en server1"
```

(Se nos indicará el nombre del fichero ssh-keygen crea un fichero id_rsa)

Tendremos así creado el par de claves en la carpeta .ssh del home:

id_jefe_server1.pub (pública)

id_jefe_server1 (privada)

Autenticación por claves

2. Copiar a clave desde o cliente ao servidor, para dar acceso:

Empregaremos o comando **ssh-copy-id** que se executará no **cliente**:

```
$ ssh-copy-id jefe@192.168.1.200
```

Que copiará o ficheiro público do usuario cliente, na carpeta `.ssh` de jefe, no servidor 192.168.1.200

Agora no servidor, no **home** de **jefe**, debe aparecer na carpeta `.ssh` un ficheiro ***authorized_keys*** coas claves públicas das identidades dixitais autorizadas para autenticarse con claves por ssh

Agora podemos conectarnos desde o cliente, ou copiar algún ficheiro:

```
$ ssh jefe@192.168.1.200
```

```
$ scp foto1.png jefe@192.168.1.200:/home/jefe
```

Conectándonos como jefe, sen necesidade de introducir contrasinal.

Autenticación por claves

CREACIÓN de novas claves **no cliente**

Podemos crear outro par de claves para outro servidor (ana en server2):

```
$ ssh-keygen -t rsa -f ~/.ssh/id_ana_server2 -C "id para ana en server2"
```

Temos creado outro o par de claves:

id_ana_server2.pub (pública)

id_ana_server2 (privada)

Teremos 4 ficheiros (2 pares) na carpeta .ssh do **home (~)** do **usuario** do cliente.

Agora teríamos que copiar de novo a clave pública para ana, no server2.

```
$ ssh-copy-id ana@192.168.1.222
```

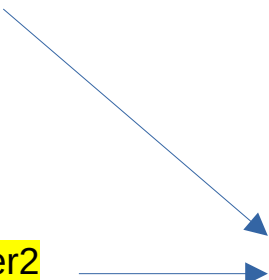
E xa nos conectaríamos como ana a server2, indicando o ficheiro de clave privada, con:

```
$ ssh -i ~/.ssh/id_ana_server2 ana@192.168.1.222
```


ssh- Cliente – Gardar Favoritos

Podemos precisar acceder por ssh a diferentes equipos, con diferente porto e diferentes usuarios e identidades dixitais. Para facilitar as cousas podemos configurar ese perfil no home do noso usuario, nun ficheiro **~/.ssh/config**. Este arquivo, coa configuración anterior:

```
Host jefe_server1
  User jefe
  Hostname 192.168.1.200
  Port 22
  PubkeyAuthentication yes
  IdentifyFile ~/.ssh/id_jefe_server1
Host ana_server2
  User ana
  Hostname 192.168.1.222
  Port 22
  PubkeyAuthentication yes
  IdentifyFile ~/.ssh/id_ana_server2
```



The diagram shows two blue arrows originating from the yellow-highlighted paths `~/.ssh/id_jefe_server1` and `~/.ssh/id_ana_server2` in the configuration block. Both arrows point towards the text 'Arquivos da clave privada' located at the bottom right of the slide.

E xa podemos conectarnos con:

```
$ ssh jefe_server1  (a server1 como jefe)
```

Ou ben:

```
$ ssh ana_server2  (a server2 como ana)
```

Arquivos da **clave privada**

SSHD- Configuración do servidor

Podemos configurar o servidor ssh editando o ficheiro **/etc/sshd_config**. Algunhas son:

- Port 25. Cambia o porto
- PasswordAuthentication yes. Permite autenticación por password. Podemos cambialo a no, cando teñamos no noso servidor ben configurada a autenticación por claves.
- PermitRootLogin yes. Permite conectarse como root. Inseguro. Debería ser usado só de forma temporal

Despois hai que reiniciar o servizo:

\$ systemctl restart ssh

ou ben

\$ service ssh restart