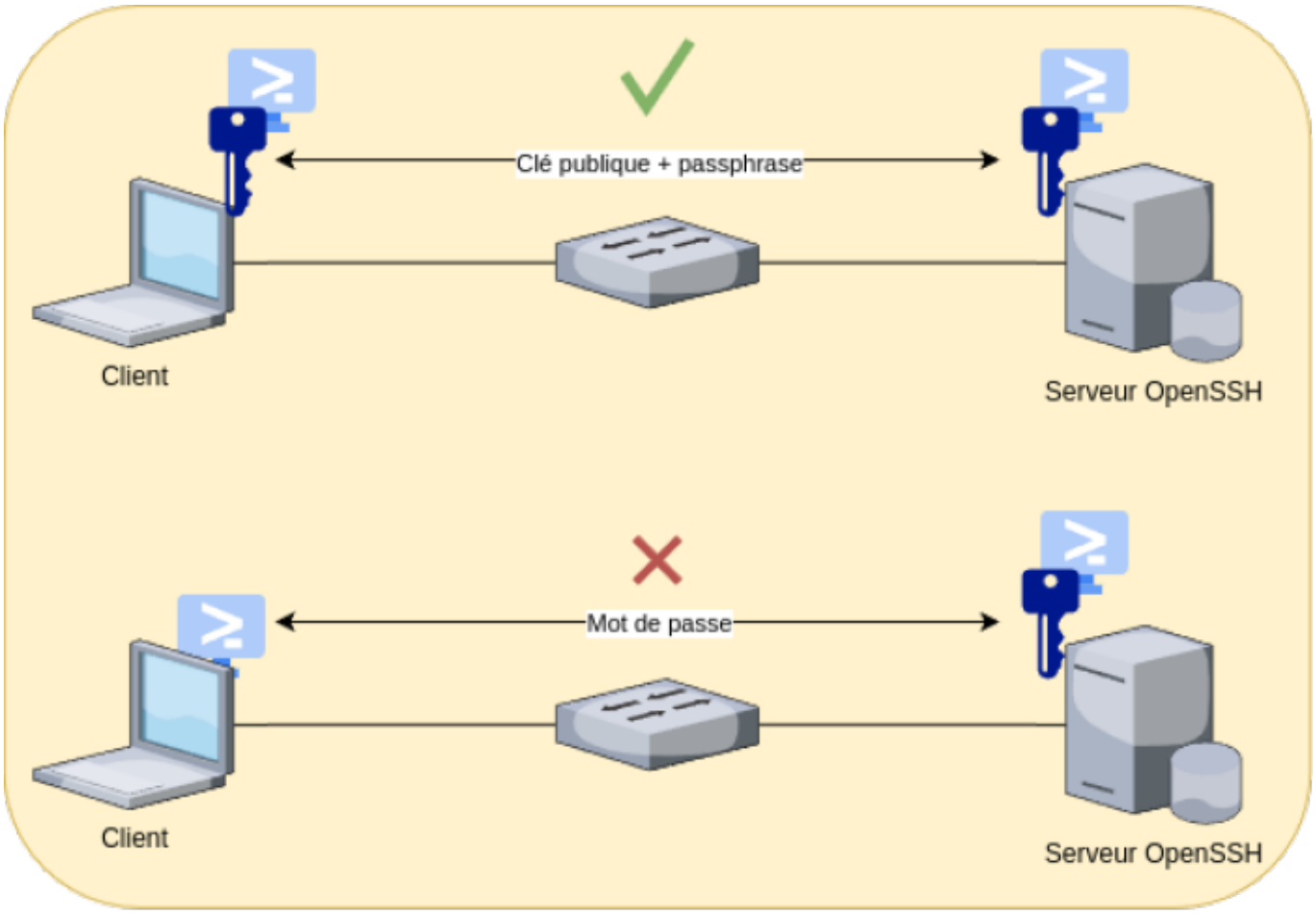
Authentification par Clé publique



Générer la clé publique

La clé doit etre générer par le client et par la suite transmit au serveur ssh.

installer le paquet OpenSSH si il ne l'est pas.

```
sudo apt install openssh-client
```

Puis générer la clé avec **ssh-keygen**.

La clé sera générer dans le dossier **/home/utilisateur/.ssh/**

```
ssh-keygen
```

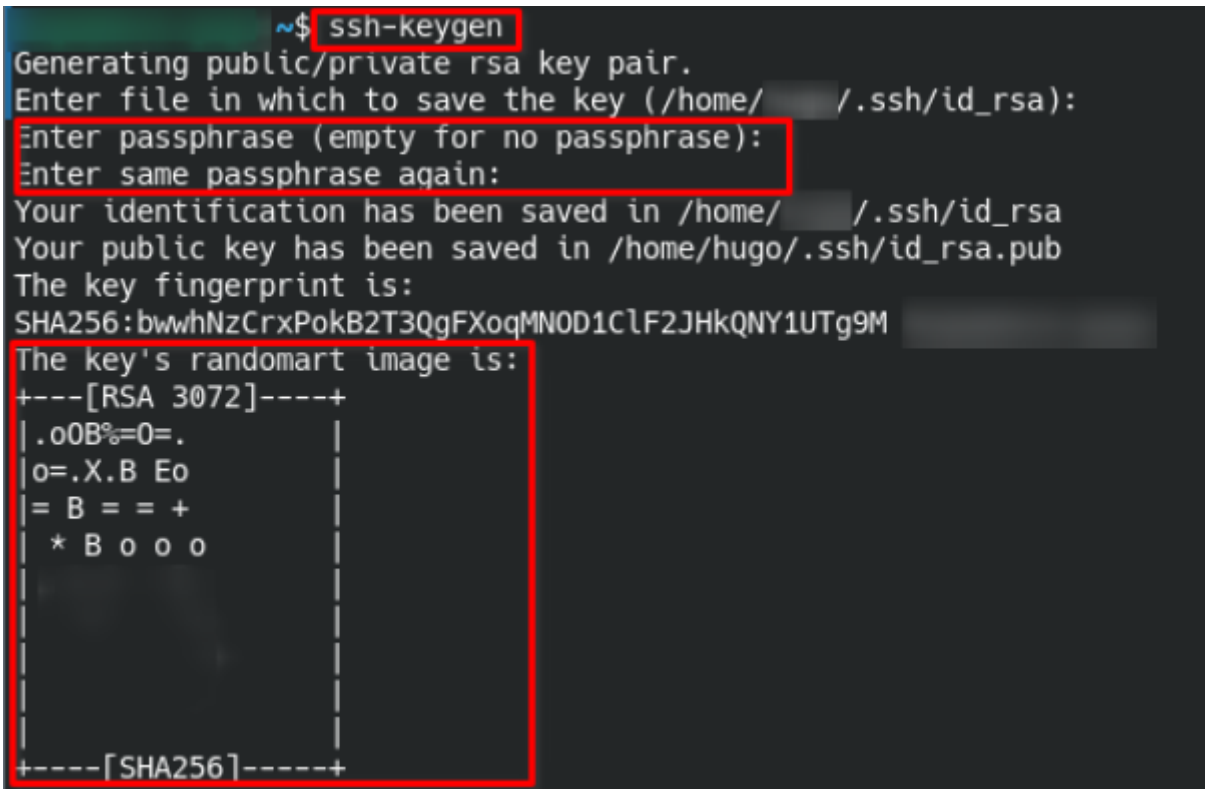
Si aucune option n'est spécifiée, une clé RSA de 2048 bits sera créée.

L'option **-b** permet de spécifier la taille.

```
ssh-keygen -b 4096
```

Afin de protéger la clé en cas de compromission, il faut définir une passphrase.

Son Fingerprint sera également afficher.



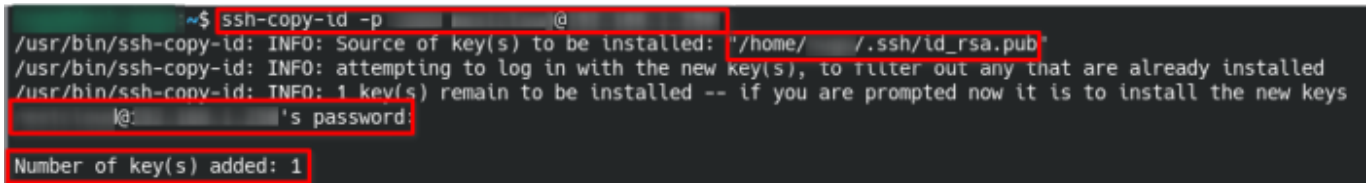
Configurer la clé sur le serveur

Avec **OpenSSH** on peut ajouter la clé avec **ssh-copy-id**.

```
ssh-copy-id utilisateur@serveur
```

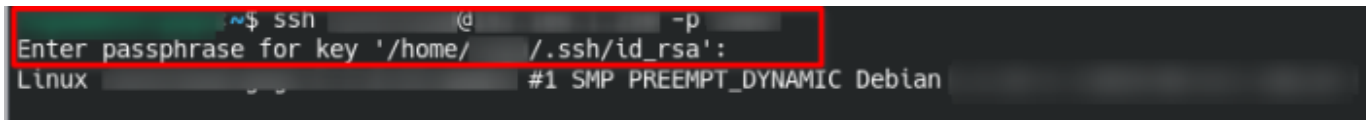
-p Pour spécifier le port.

```
ssh-copy-id -p 500 utilisateur@serveur
```



Il faudra spécifier le mot de passe une dernière fois.

La connexion avec ce client se fera désormais avec la passphrase.



Désactiver la connexion par mot de passe

Éditer le ficher **/etc/ssh/sshd_config**.

```
sudo vim /etc/ssh/sshd_config
```

Éditer ces 2 lignes :

```
PasswordAuthentication no
PubkeyAuthentication yes
```

Puis relancer le service **sshd**.

```
sudo systemctl restart sshd
```