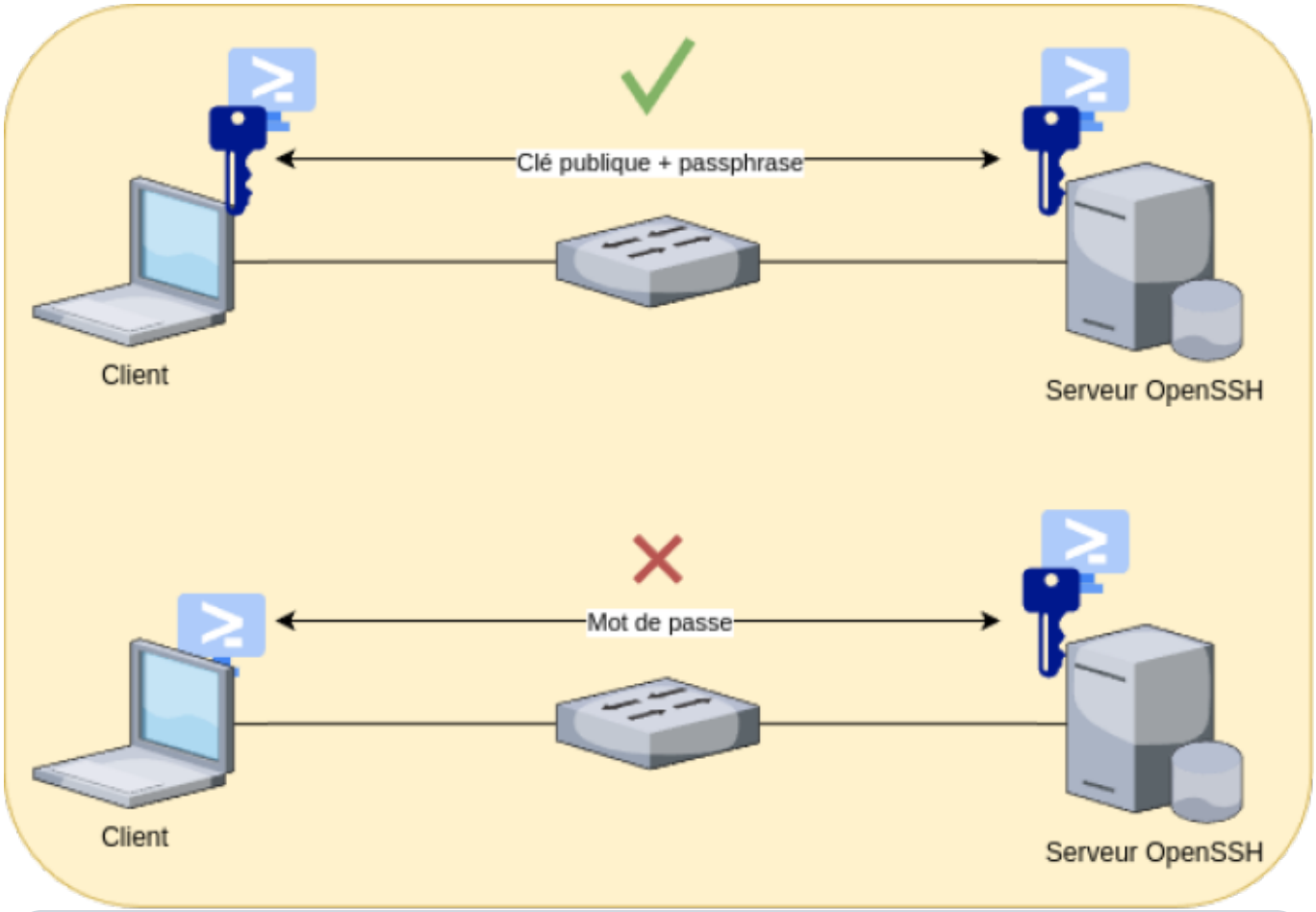
Authentification par Clé publique

L'authentification **SSH** par **clé** permet de choisir les clients **autorisés** à se connecter sur le serveur SSH. Mais l'intérêt est aussi de pouvoir tous les **désactiver** en retirant la clé de **confiance** sur le serveur.



Sources importantes

- Article IT-Connect : Authentification SSH par clés
- Article DigitalOcean : Comment configurer une authentification par clé SSH sur un serveur Linux

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
```

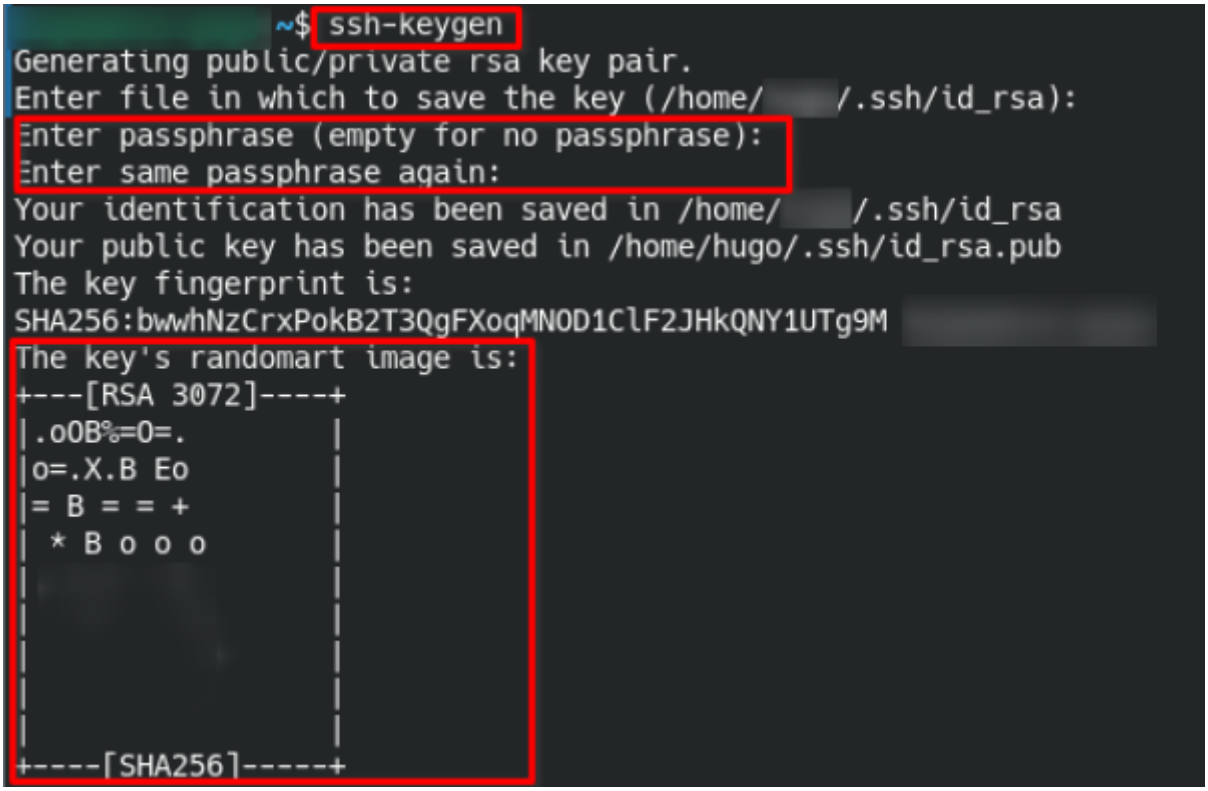
Si aucune option n'est spécifiée, une clé RSA de 2048 bits sera créée.

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.



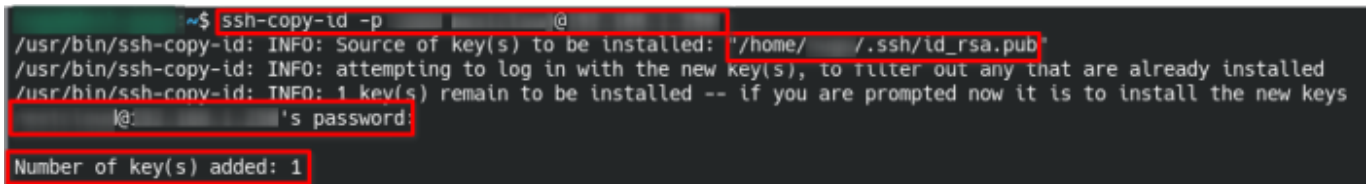
Configurer la clé sur le serveur

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

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

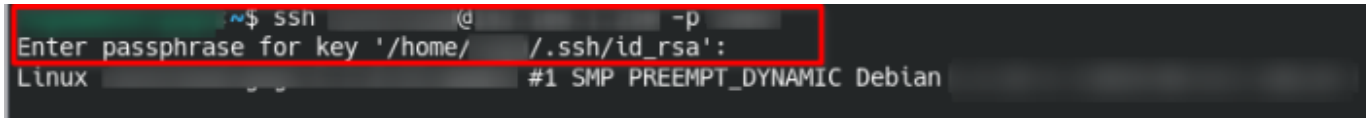
-p Pour spécifier le port.

```
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.



La clé est désormais stocker sur le serveur dans le dossier .**ssh** de l'utilisateur connecté.

~/.ssh (vérifier la permission du dossier en **700**)

Et la liste des clés autoriser dans lee fichier **authorized_keys**.

~/.ssh/authorized_keys (vérifier la permission du fichier en **600**)

Désactiver la connexion par mot de passe

Avant de désactiver la connexion par mot de passe, s'assurer qu'au moins un client peut se connecter par clé.

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
```

Désormais seul les clients possédant la clé peuvent se connecter, les autres auront le message (Permission denied)

Debugger la connexion

Activez le mode verbose sur le client pour déboguer :

```
ssh -vv user@server
```