Table des matières

Avant-Propos

E6 :

Elaboration de documents relatifs à la production et à la fourniture de services
A1.1.1 , Analyse du cahier des charges d'un service à produire
A1.2.4 , Détermination des tests nécessaires à la validation d'un service
A1.3.4 , Déploiement d'un service
A4.1.9 , Rédaction d'une documentation technique

Installation et configuration

Pour installer le SSH, il faut taper la commande suivante :

```
root@debian:~# apt-get install ssh_
```

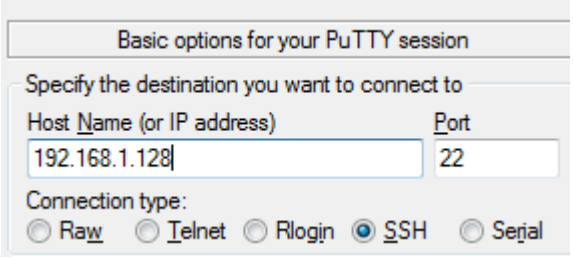
Par défaut, le serveur ssh est configuré pour une authentification par mot de passe. Pour changer cela, il faut modifier le fichier /etc/ssh/sshd_config avec l'éditeur nano et rajouter les lignes, ou plus particulièrement les décommenter :

```
PubkeyAuthentication yes
AuthorizedKeysFile      %h/.ssh/authorized_keys
```

On redémarre ensuite le service :

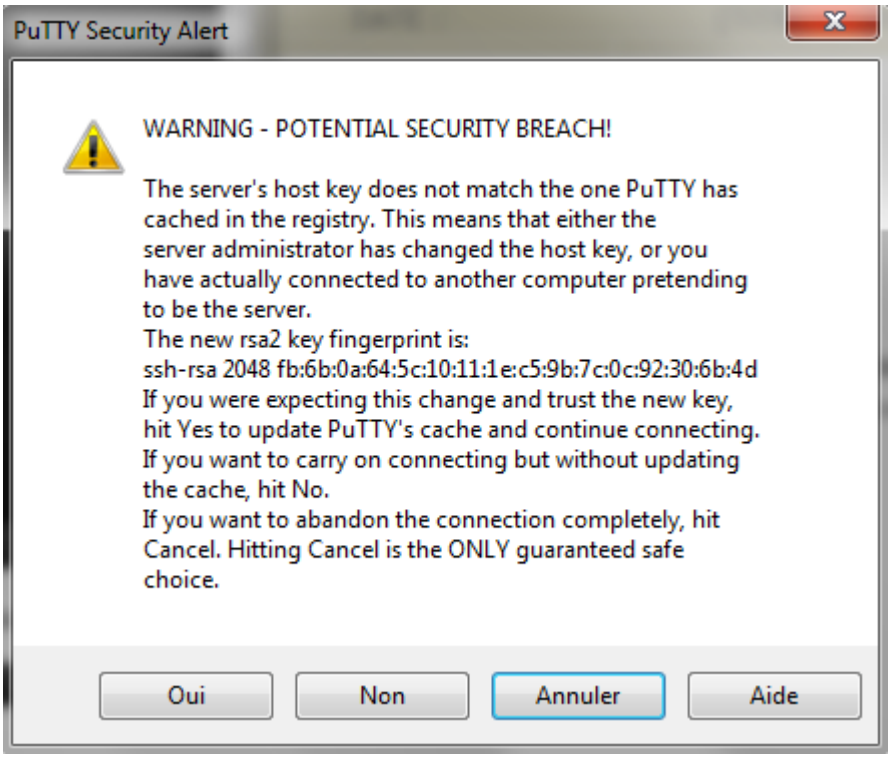
```
root@debian:~# service ssh restart
```

Maintenant, on peut se connecter en SSH :



La première fois que l'on se connecte en SSH, un message d'alerte apparait.

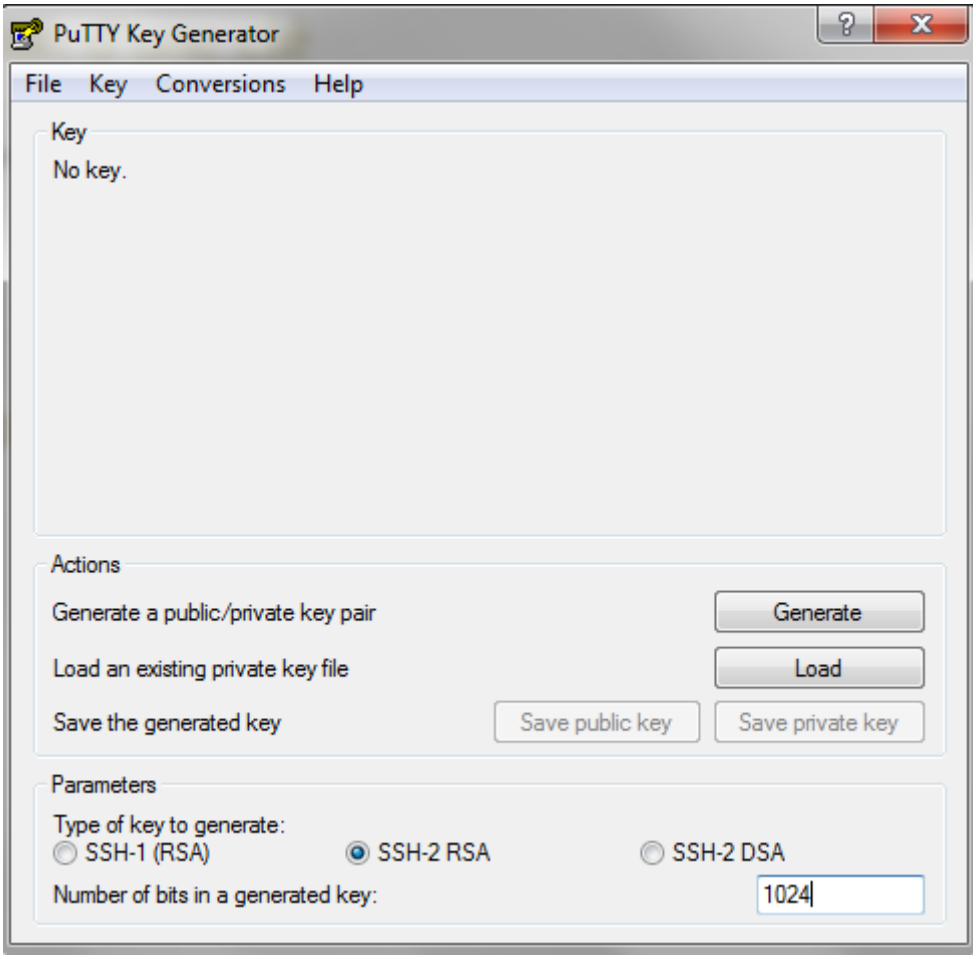
On clique sur oui, pour mémoriser la clé publique dans la base de registre Windows.



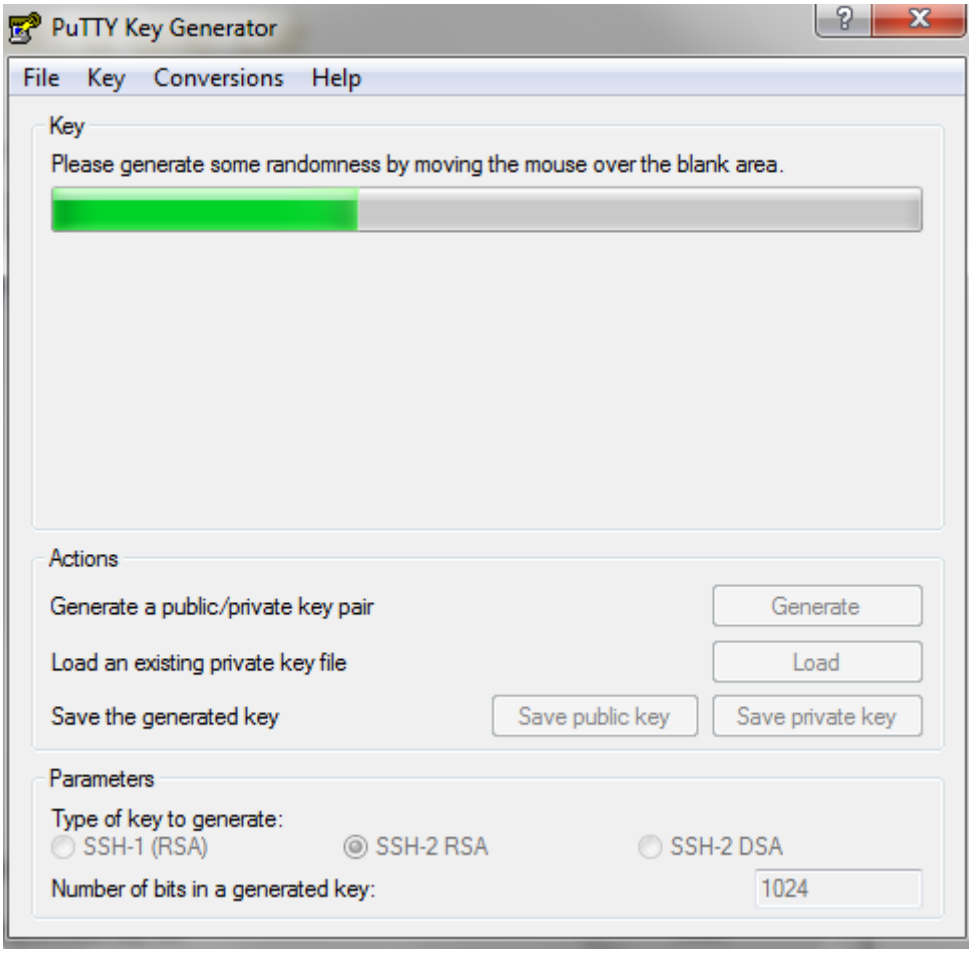
C'est une clé publique, le serveur est propriétaire de la clé, et elle est transmise afin que le client puisse se connecter.

Génération d'une clé

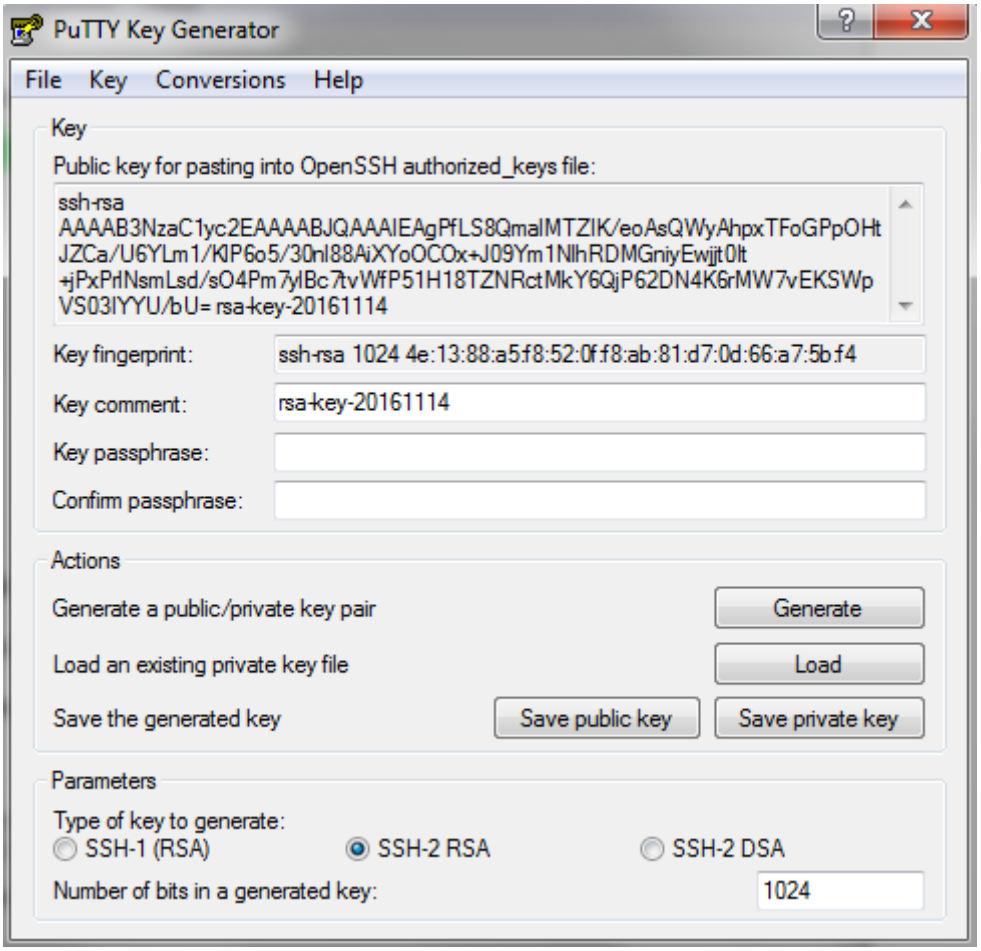
Pour créer une clé, il faut lancer l'utilitaire PuTTYgen



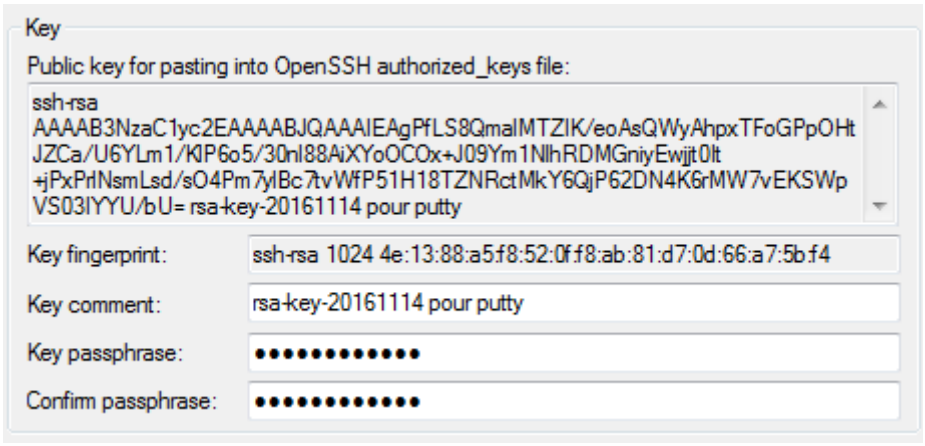
On choisit le paramètre le nombre de bit puis on clique sur générer.



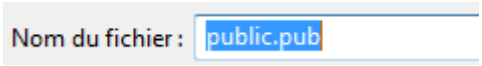
Il faut secouer la souris sur la fenêtre afin que la génération avance.

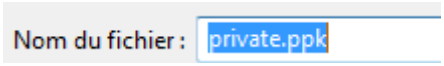


Il faut ensuite ajouter un mot de passe, parce que c'est plus sécurisé.



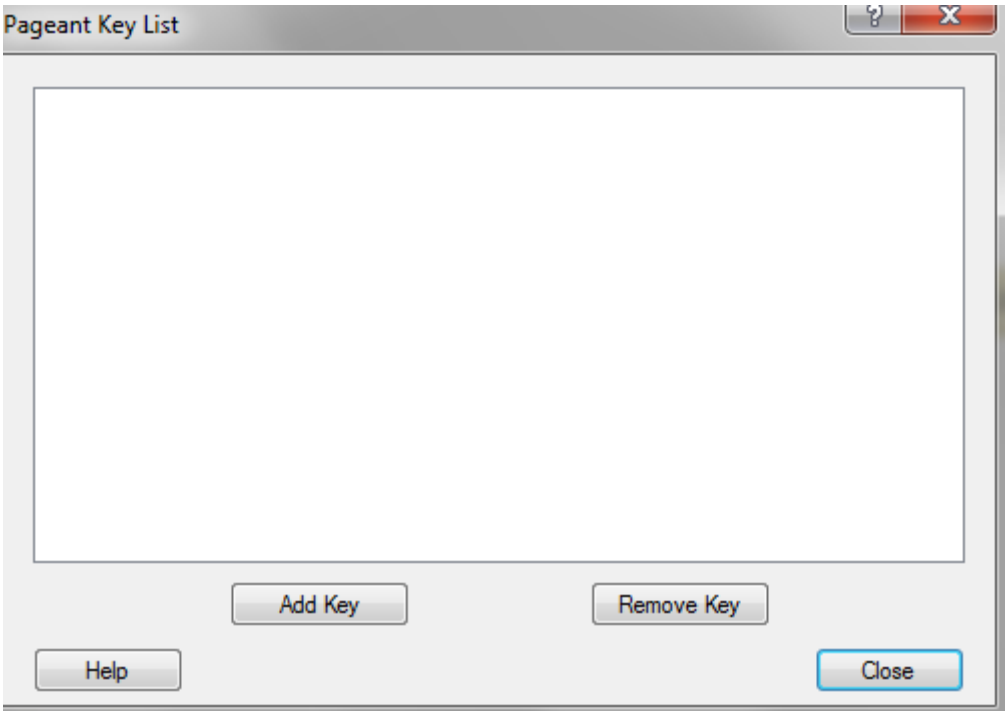
Une fois que l'on à tout bien paramétré, il faut enregistré la clé publique et la clé privée. On clique donc sur Save public key et Save private key.
Attention, la clé privée doit avoir une extension .ppk et la clé publique une extension .pub



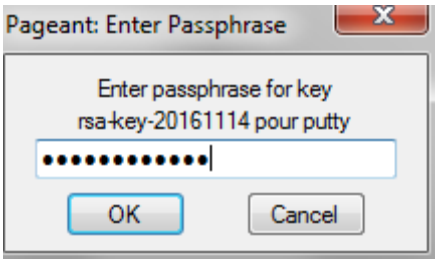


Nous avons donc généré une clé privée et une clé publique. Il faut bien entendu protéger et éviter de transmettre la clé privée.

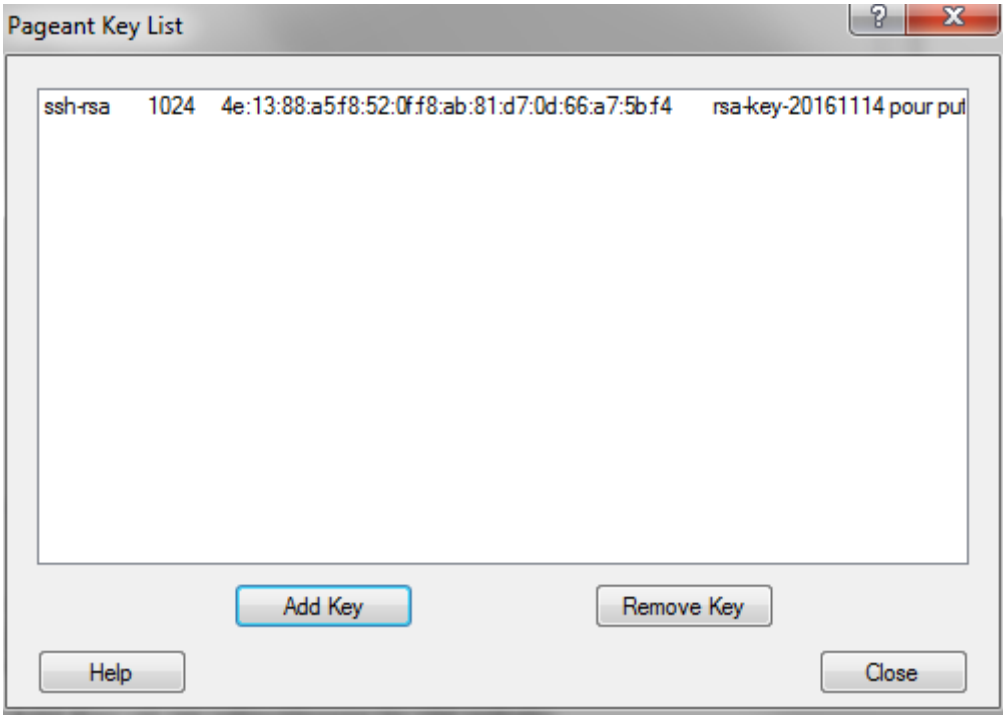
Pour charger la clé, il faut lancer le logiciel Pageant.



On clique sur Add Key et on sélectionne la clé privée.

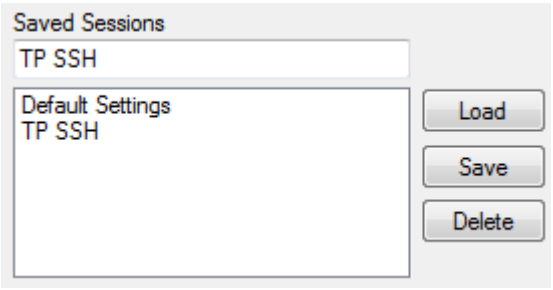


On rentre le mot de passe que l'on a mis précédemment (dans mon cas j'avais mis Password1234)

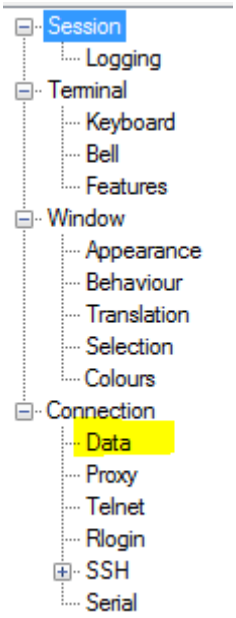


Une fois que la clé est ajoutée on peut fermer l'utilitaire.

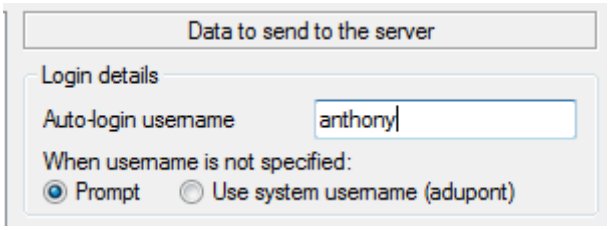
On lance maintenant putty et on créer une session, il suffit de marquer l'adresse IP et de lui donner un nom :



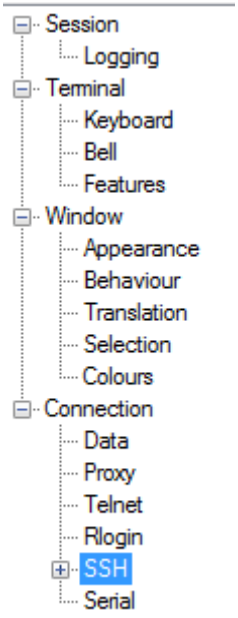
Une fois que cela est fait on choisit la session en cliquant dessus puis on va dans DATA dans le menu à droite.



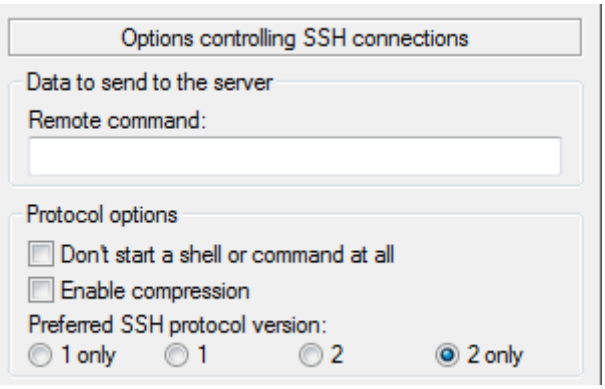
Puis il faut ajouter le nom du compte sur lequel on veut se connecter :



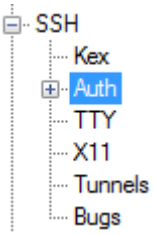
Ensuite on va dans le menu SSH



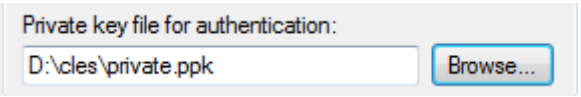
Puis on choisit le bouton radio 2only



Maintenant on va dans le sous-menu du SSH « Auth »



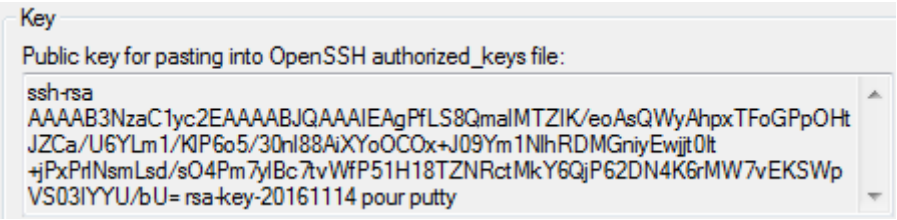
Puis on choisit le fichier de la clé privé que l'on veut utiliser.



Puis on retourne sur session et on clique sur Save.

Une fois que putty est configuré, nous allons paramétrer la clé publique sur le serveur.

Il faut relancer l'utilitaire puTTYgen, cliquer sur le bouton load et charger la clé privée et rentrer le mot de passe.



Il faut ensuite copier ce qui est marqué ici dans le presse papier.

On démarre la session putty et on se connecte sur l'utilisateur qui est créé sur la machine.

Ensuite, sur le serveur, dans le home de l'user, on créer un dossier ssh.

```
anthony@debian:~$ mkdir .ssh
```

On copie ensuite le contenu du presse papier dans un fichier qui s'appelle authorized_keys

```
anthony@debian:~$ cat >> .ssh/autorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAIEAgPfLS8QmalMTZIK/eoAsQWyAhpxTFoGPpOHtJZCa/U6Y
Lm1/KlP6o5/30nl88AiXYoOCOx+J09Ym1NlhRDMGniyEwjjt0It+jPxPrlNsmLsd/sO4Pm7ylBc7tvWf
P51H18TZNRctMkY6QjP62DN4K6rMW7vEKSWpVS03IYYU/bU= rsa-key-20161114 pour putty
```

Donc, pour ce faire, on fait le cat, puis une fois que la commande est lancée on fait shift + ins sur le clavier ce qui va copier le presse papier, puis on appuie sur Entrée et enfin on fait un ctrl + d pour fermer le cat.

On modifie ensuite les droits sur le répertoire home (lecture, écriture et exécution par le propriétaire seul, à l'exclusion de tout autre)

```
anthony@debian:~$ chmod u+rwx,g+---,o+--- /home/anthony
```

Puis on modifie les droits sur le fichier .ssh/autorized_keys. On donne les droits de lecture/ecriture uniquement, par le propriétaire seul à l'exclusion de tous les autres.

```
anthony@debian:~$ chmod u+rw-,g+---,o+--- .ssh/autorized_keys
```