

# Configurer une authentification avec un couple de clés privée/publique SSH

## Présentation

Pour administrer un serveur Linux, vous pouvez utiliser le compte **root** ou, ce qui est fortement conseillé, un compte que vous avez créé et à qui vous avez permis une **élévation de privilèges**.

Si vous gérez un autre serveur, il est également fortement conseillé d'utiliser **un mot de passe différent**. Cette solution n'est **pas satisfaisante et peu sécurisée** si vous devez gérer de nombreux serveurs.

Par ailleurs cela est problématique si vous avez des tâches d'administration à **automatiser** car la saisie manuelle du mot de passe sera nécessaire ou bien il faudra indiquer le **mot de passe dans les scripts** ce qui est problématique si vous n'avez pas de solution pour les chiffrer. Les solutions possibles :

- utiliser un **annuaire LDAP pour centraliser** la gestion des comptes.
- utiliser des **clés SSH publique**.

Vous aller configurer le compte **root** ou le compte linux que vous avez créé afin de permettre d'ouvrir une session en utilisant une **clé publique SSH**. Vous utiliserez **votre propre clé publique SSH** pour vous connecter. Vous permettrez à l'enseignant de se connecter en simple utilisateur avec un compte que vous devez créer et appeler ensbtssio avec sa **clé publique SSH**.

Après la création de votre **couple de clés Privée/publique**, communiquez aux enseignants votre **clé publique** dans le dossier partagé Classe.

Votre clé publique sera rajoutée à la page des clés SSH du BTS SIO à la page :

- [Les clés publiques SSH Etudiant/enseignants](#)

- En utilisant **mot de passe**, vous utilisez **un seul facteur** d'authentification.
- En utilisant une **clé publique SSH**, vous utilisez également **un seul facteur** d'authentification.



Cependant, vous pouvez utiliser la **même clé publique SSH sur plusieurs serveurs** en ne retenant qu'un seul mot de passe, celui de la passphrase de votre clé privée.

En général on **désactive** ensuite l'authentification par mot de passe sur les serveurs afin de n'autoriser que l'authentification par clé SSH publique.

Pour en savoir plus : <https://www.it-connect.fr/chapitres/authentification-ssh-par-cles/>

## Générer une paire de clé SSH depuis un client OpenSSH

Générer une paire de clés privée/publique depuis un client Windows ou linux.



Il est conseillé de protéger l'utilisation de la clé privée avec une passphrase.

```
$ ssh-keygen
```

```
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/centrecallbd/.ssh/id_rsa):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/centrecallbd/.ssh/id_rsa.  
Your public key has been saved in /home/centrecallbd/.ssh/id_rsa.pub.  
The key fingerprint is:  
SHA256:0rjedyVuT2fzEJHgw5I9lfmTsQ6MHSD87Xrr/aXE3r4 centrecallbd@Ch2Lab1  
The key's randomart image is:  
+---[RSA 2048]---+  
|                .. .o .o |  
|                ..= +oo |  
|                + @ +.+ |  
|                o  + B =. |  
|                o S  . + . |  
|                o   .o.o |  
|                .   ..0=.+ |  
|                . .  ..+=.*+ |  
|                . .  oo+=EB |  
+-----[SHA256]-----+  
$
```

Dans le dossier caché **.ssh** (sous Windows Linux ou MacOSX) vous avez votre couple de clés privée (id\_rsa) et publique (id\_rsa.pub).

```
$ ls .ssh  
id_rsa  id_rsa.pub  
$
```



Un autre fichier **known\_hosts** sera ensuite créé dans le dossier **.ssh** afin de contenir **les clés publiques des serveurs** sur lesquels vous vous êtes authentifié avec un mot de passe ou une clé SSH publique. bloc information

## Configurer un accès SSH avec une clé SSH depuis un client OpenSSH

- Copiez ensuite votre clé publique sur le serveur auquel vous souhaitez accéder avec la clé SSH.

```
$ ssh-copy-id utilisateur@IP_ordinateur_cible
```



La clé publique est copiée dans le fichier **.ssh/authorized\_keys** du serveur distant.

La commande `ssh-copy-id` n'est pas disponible sous Windows. Vous pouvez alors :



- utiliser la commande **scp** pour copier le fichier `id_rsa.pub` dans le dossier l'utilisateur ;
- ouvrir une session ssh pour pouvoir ensuite ajouter le contenu du fichier `id_rsa.pub` dans le fichier `authorized_keys` :

```
C:> scp .ssh/id_rsa.pub  
compteutilisateur@adresseip:/home/compteutilisateur/  
C:> ssh compteutilisateur@adresseip  
$ cat id_rsa.pub >> .ssh/authorized_keys
```

Vous devez maintenant pouvoir vous connecter sans mot de passe au serveur distant :

```
$ ssh utilisateur@IP_ordinateur_cible
```

Il est fortement conseillé ensuite de désactiver l'authentification par mot de passe en modifiant le fichier de configuration du service ssh sur le serveur distant **/etc/ssh/sshd\_config** :

- Décommentez la ligne suivante en mettant sa valeur à **no** :

```
PasswordAuthentication no
```

- sauvegardez le fichier **/etc/ssh/sshd\_config** et relancer le service ssh :

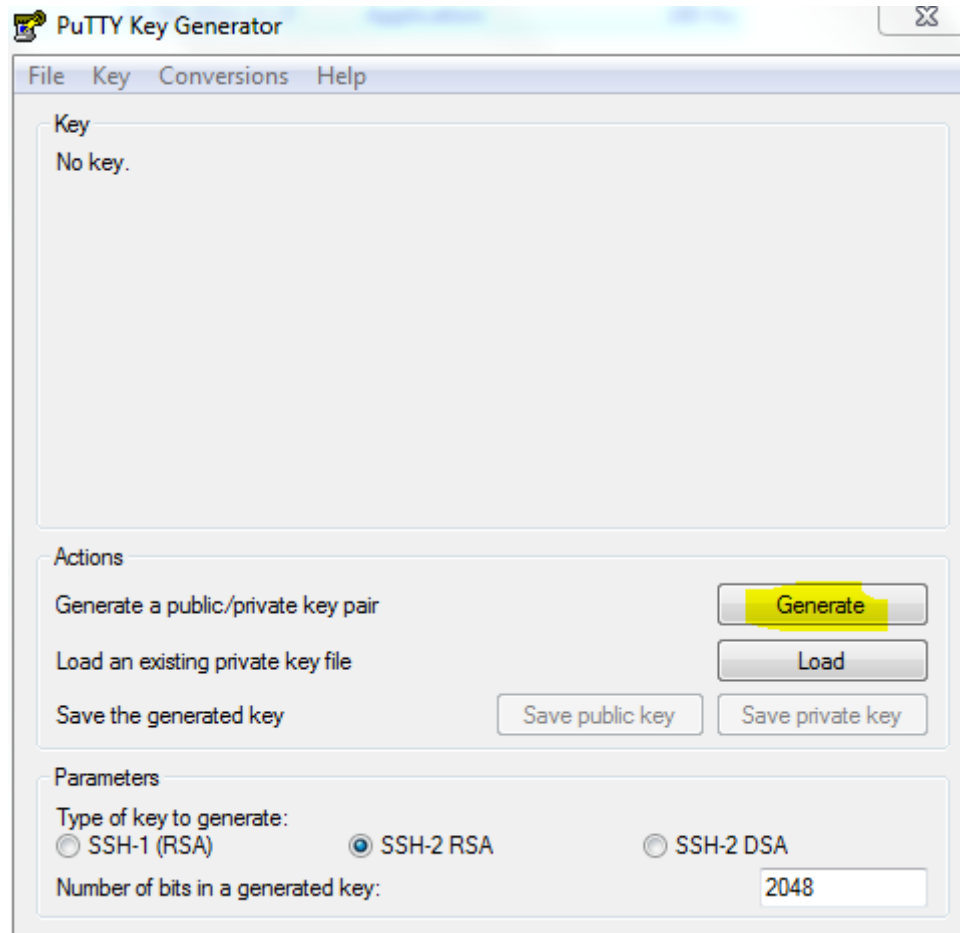
```
$ sudo systemctl restart ssh
```

Pour en savoir plus :

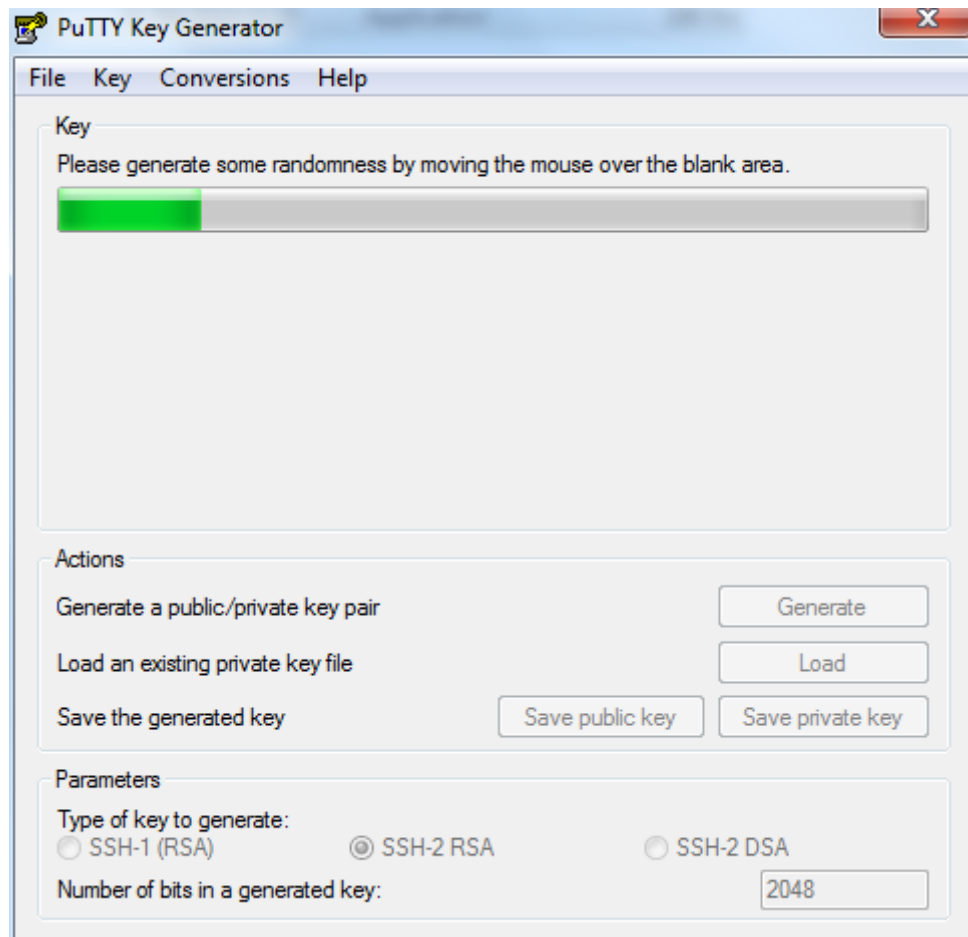
- [https://fr-wiki.ikoula.com/fr/CI%C3%A9\\_SSH-\\_comment\\_cr%C3%A9er\\_une\\_cl%C3%A9\\_SSH\\_\(Debian\\_10\)](https://fr-wiki.ikoula.com/fr/CI%C3%A9_SSH-_comment_cr%C3%A9er_une_cl%C3%A9_SSH_(Debian_10))

## Génération des clés avec PuttyGen

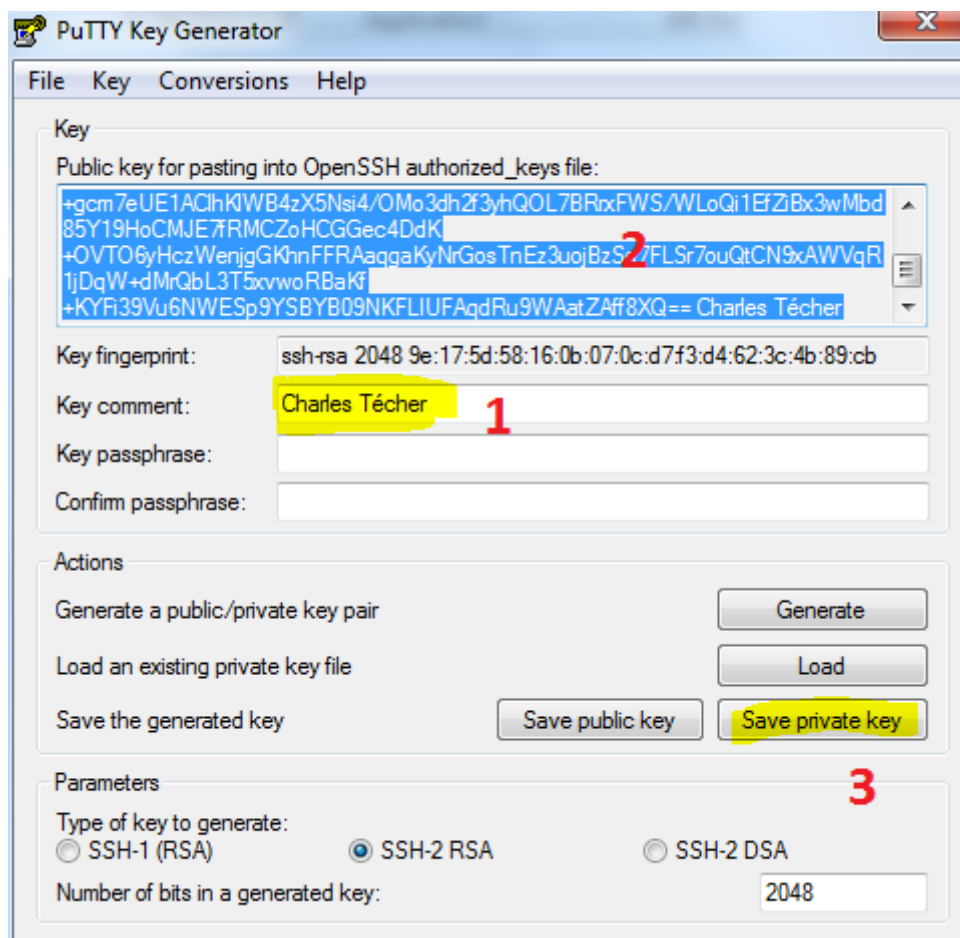
- L'utilitaire **Puttygen** est disponible à l'adresse [PuttyGen](#). IL est disponible dans le **dossier partagé de la classe**.
- Lancez PuttyGen



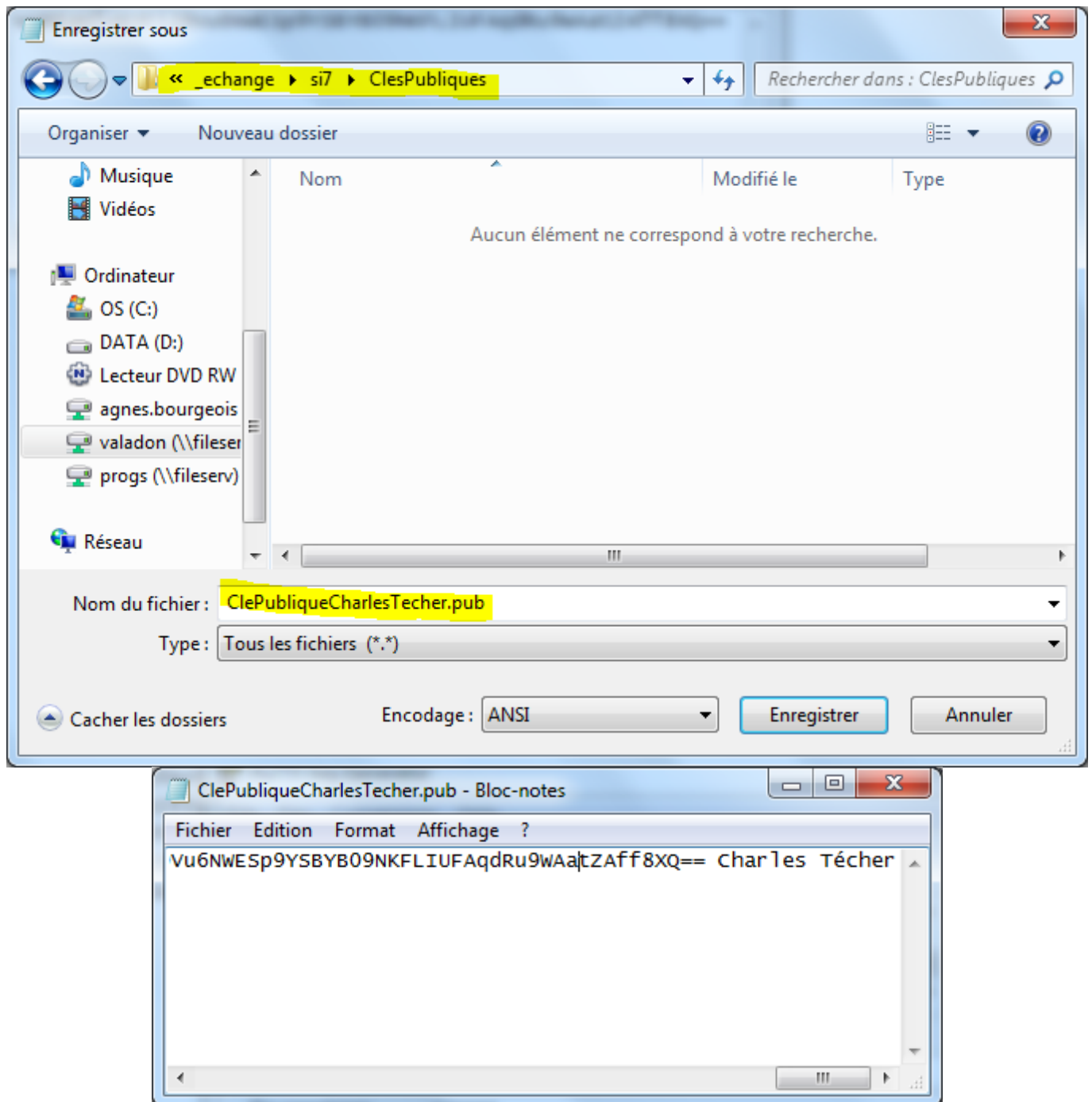
- Cliquez sur le bouton **Generate** et bouger la souris sur la **zone blanche**.



- Mettez **votre nom** comme commentaire de la clé publique.
- Sélectionnez puis Copiez/Collez votre clé publique dans un fichier texte (extension **.pub**) dans votre dossier personnel.
- Cliquez sur le bouton **Save private key** pour enregistrer votre clé privée (extension **.ppk**) dans votre dossier personnel.

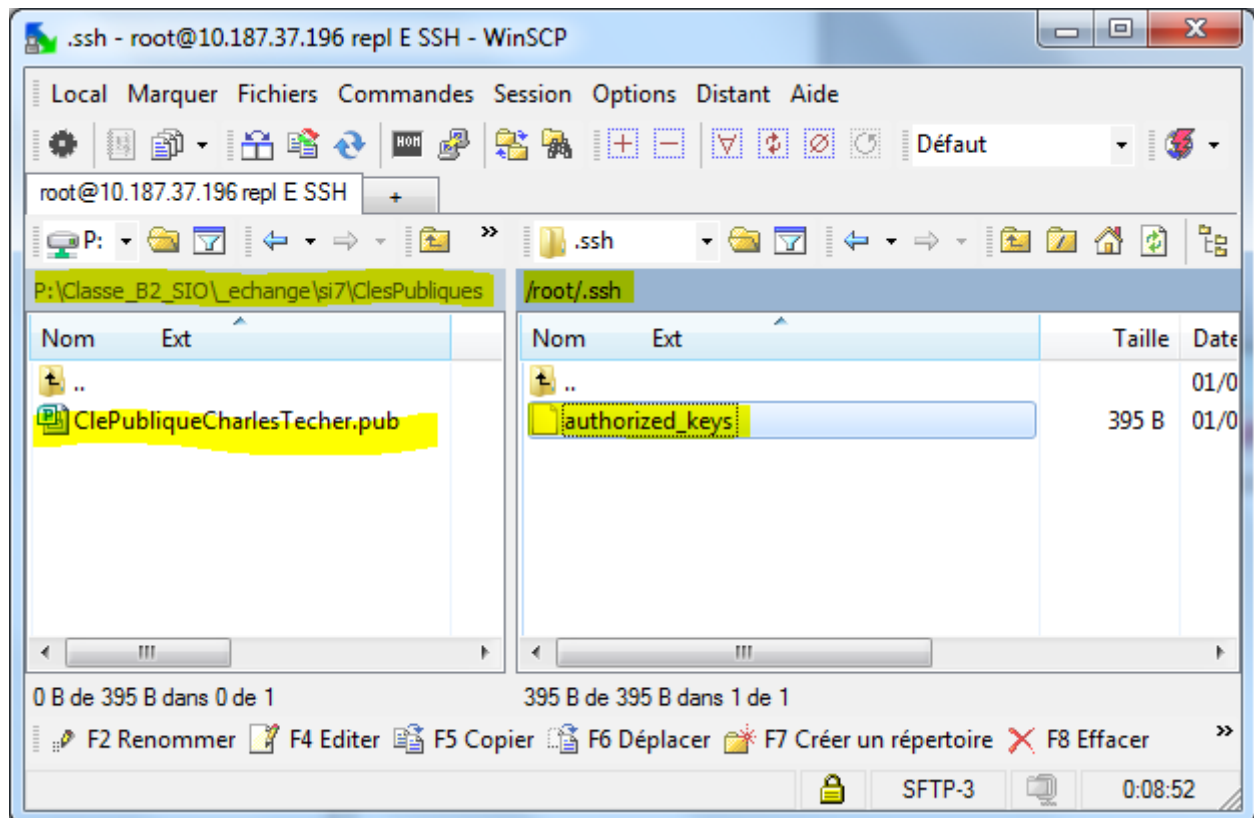


- Le contenu du fichier de votre clé publique



## Configuration de l'accès SSH

- Utilisez **WinSCP** pour vous connecter avec le compte **root** sur votre VM Debian.
- Créez dans le dossier **/root** un dossier **.ssh** et un fichier **/root/.ssh/authorized\_keys**

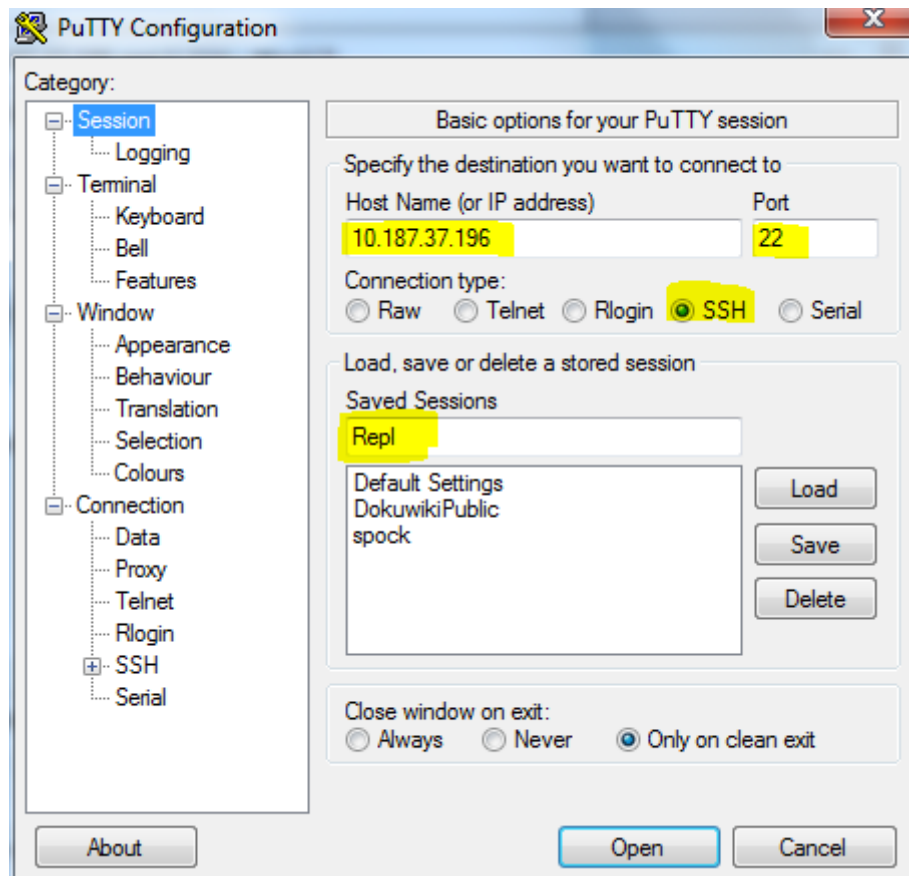


- Copiez dans ce fichier le contenu de votre **clé publique**.
- Créez dans le dossier du compte **/home/ensbtssio** un dossier **.ssh** et un fichier **/home/ensbtssio/.ssh/authorized\_keys**
- Copiez dans ce fichier la **clé publique** de l'enseignant disponible depuis la page [Les clés publiques SSH Etudiant/enseignants](#).

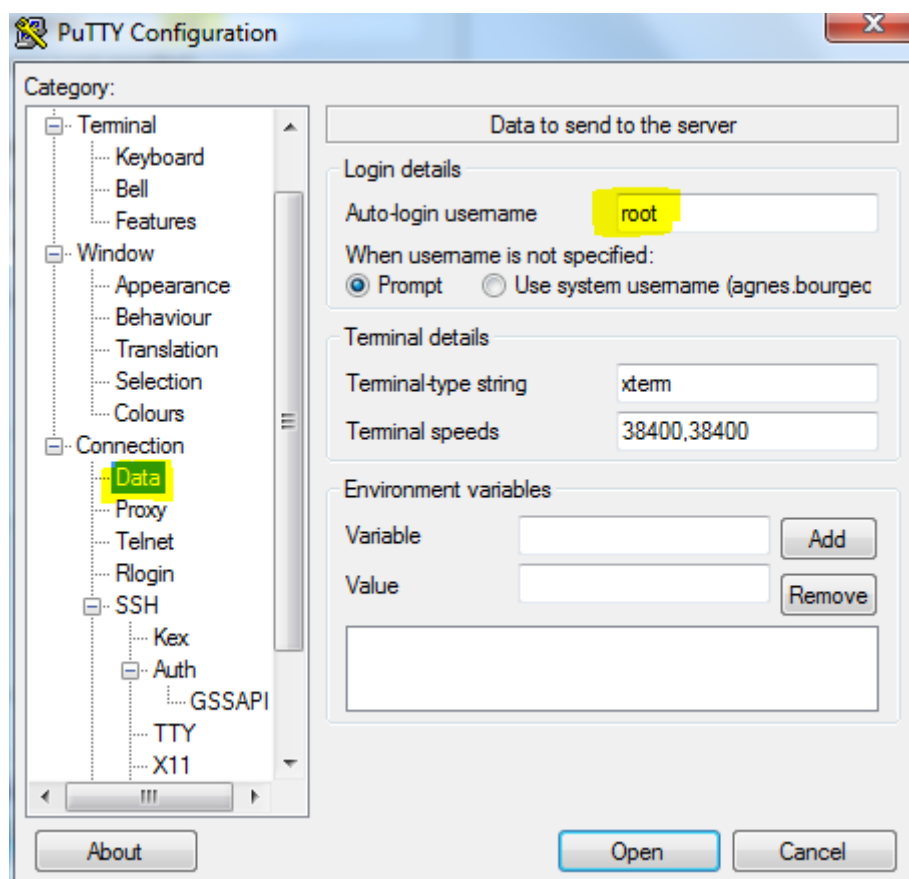
## Accès au serveur en SSH avec Putty

- Configurez Putty pour avoir un accès **console** à votre serveur.
- Indiquez l'**adresse IP** de votre serveur et le **port 22 (SSH)**.

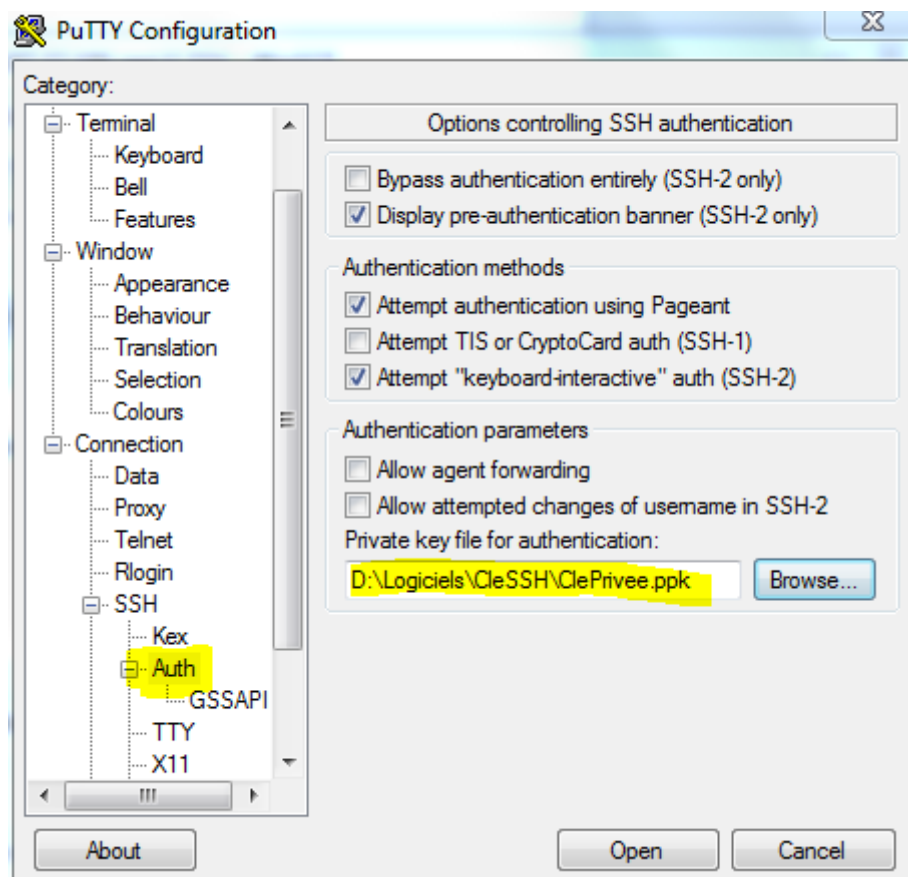




- précisez le compte **root** pour vous connecter :



- précisez votre **clé privée**



From:  
<https://siocours.lycees.nouvelle-aquitaine.pro/> - Les cours du BTS SIO

Permanent link:  
<https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/reseau/debian/clessh?rev=1637528994>

Last update: 2021/11/21 22:09

