

Connexion au serveur sesame-mips

[source : <http://doc.fedora-fr.org/wiki/SSH : Authentification par cl%C3%A9>]

Pour vous connecter sur le serveur de l'université, vous devez utiliser une connexion sécurisée par clefs (asymétriques : une public et une privée).

~/ fait référence à votre dossier personnel sur le serveur de l'université (machine sur laquelle vous voulez vous connecter)

~chezvous/ fait référence à votre dossier personnel sur votre machine (à partir de laquelle vous voulez vous connecter sur le serveur de l'université)

Chaque connexion SSH vérifie l'identité du serveur (par sa clé d'hôte ~chezvous/.ssh/known_hosts) puis celle du client (par mot de passe ou clé publique ~/.ssh/authorized_keys).

La première étape est donc de générer les clefs. Ces clefs seront définies par une « passphrase » (un mot de passe long) qui sera différent de votre mot de passe habituel. C'est cette passphrase qu'il faudra taper (éventuellement selon les configurations) pour vous connecter.

ssh-keygen

C'est la commande sous linux pour générer les deux clefs. ssh-keygen a plusieurs options qui ne seront pas évoquées ici.

Résultat : création d'une clef privée (id_rsa) à mettre de là où on se connecte et d'une clef public (id_rsa.pub) à utiliser là où on veut se connecter.

```
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (~/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in ~/.ssh/id_rsa.
Your public key has been saved in ~/.ssh/id_rsa.pub.
The key fingerprint is:
cb:61:48:6b:b4:53:00:9b:d1:2a:cf:44:88:79:c2:19 login@olivier
```

Tapez entrée (laissons la valeur par défaut)

Tapez votre passphrase puis entrée, il n'y a pas de caractère qui s'affiche à l'écran

Deux fichiers ont été créés (dans le dossier ~/.ssh/) :

- id_rsa: contient la clé privée et ne doit pas être dévoilé ou mis à disposition
- id_rsa.pub : contient la clé publique, c'est elle qui sera mise sur les serveurs dont l'accès est voulu.

Utilisation de la clef publique

Il faut ajouter la clef publique aux clefs autorisées pour la connexion.

```
login@olivier ~> cd .ssh
login@olivier ~/.ssh> cat id_rsa.pub >> authorized_keys
```

Si le fichier `authorized_keys` n'existe pas encore, utilisez un seul >

Utilisation de la clef privée (en ligne de commande)

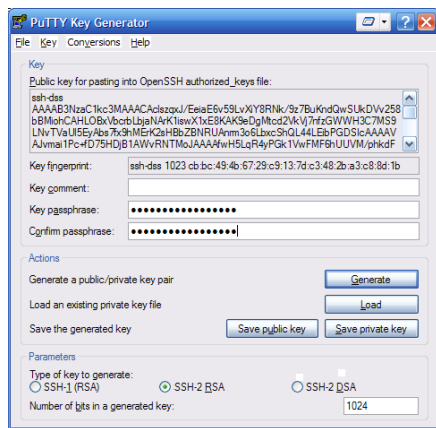
Il vous faudra donc votre clef privée (fichier `id_rsa`). Vous pouvez la placer chez vous (`~chezvous/.ssh`) si vous êtes sous linux. Le programme « `ssh` » l'utilisera par défaut. Vous pouvez aussi avoir plusieurs clefs, auquel cas vous pouvez préciser (en ligne de commande) quel fichier « `clef` » vous utilisez avec l'option `-i`.

Utilisation de la clef avec windows

conversion de la clef privée avec putty (pour windows)

Les logiciels sur windows auront besoin d'une conversion de la clef privée. Cette conversion peut se faire avec `puttygen.exe`, programme téléchargeable, gratuit, qui va avec `putty` :

<http://www.putty.org/>



Il vous faudra la clef privée (fichier `id_rsa`), donc prenez la sur une clef USB par exemple.

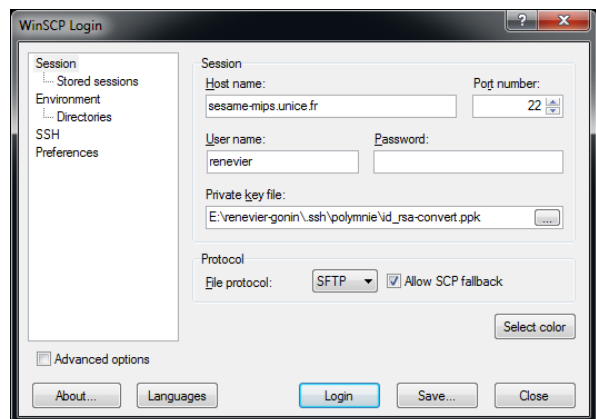
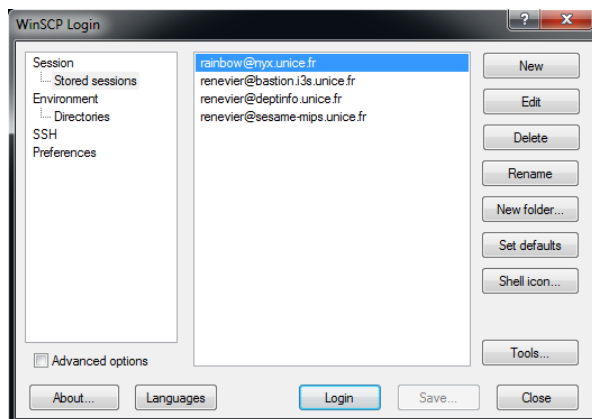
Il faut ensuite convertir cette clef au format putty. Pour cela, lancez « `Putty Secure Key Generator` » (`puttygen.exe`), puis choisissez `Conversions, Import key`.

Dans l'explorateur de fichier, sélectionnez la clef privée, la passphrase sera demandée.

Pour terminer cliquez sur « `Save Private Key` ». Choisissez le dossier et le nom du fichier pour sauvegarder la clef convertie. On aura donc une clé au format `.ppk` (Putty Private Key).

Configuration exemple pour windows

L'exemple ci-dessous utilise `winscp` (<http://winscp.net/>) mais d'autres sont possibles (Filezilla, etc.)



Vous pouvez donc enregistrer des sessions (bouton « New »).

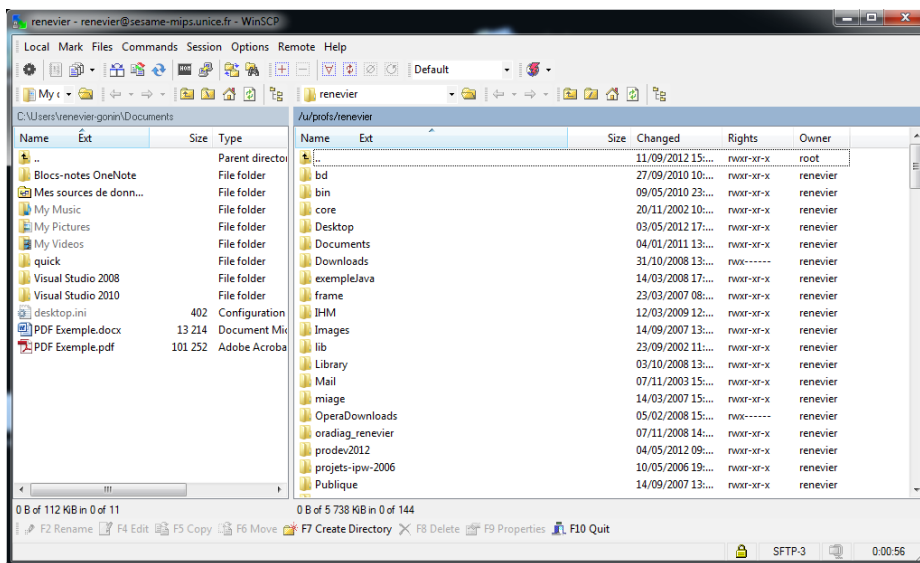
Il faut donc préciser :

- le nom du serveur (Host Name) : sesame-mips.unice.fr
- votre login (vos initiales + la fin de votre numéro étudiant)
- pas besoin de password
- indiquez où vous avez sauvegardé la clef privée convertie avec puttygen

Vous pouvez alors sauvegarder cette session et l'utiliser pour vous connectez (bouton « Login »).

Votre passphrase sera demandée.

Une fois connecté, vous verrez une fenêtre comme celle ci-dessous :



La partie gauche correspond aux fichiers sur votre ordinateur. La partie droite correspond aux fichiers qui sont sur le serveur de l'université (sur votre compte). Vous pouvez alors consultez les différents fichiers, les récupérer, en déposer (voire écraser des fichiers), en supprimer, en éditer, etc.

En particulier, vous avez le dossier www qui correspond à votre site web...