

Direction du Système d'Information (DSI)

Procédure de Création et utilisation des clefs SSH sous Windows

Sommaire

1	INTRODUCTION.....	3
2	CONTEXTE	4
3	TELECHARGEMENT ET INSTALLATION DES OUTILS.....	5
4	GENERER DES CLEF RSA	6
5	SAUVEGARDE DES CLEFS.....	8
5.1	La clef publique	8
5.2	La clef privée.....	9
6	AJOUT DE LA CLEF DANS PUTTY.....	10
7	AJOUT DE LA CLEF DANS FILEZILLA	12

1 Introduction

Ce document présente la génération de clefs d'authentification SSH pour Windows, et leur implémentation avec les outils gratuit Putty et FileZilla.

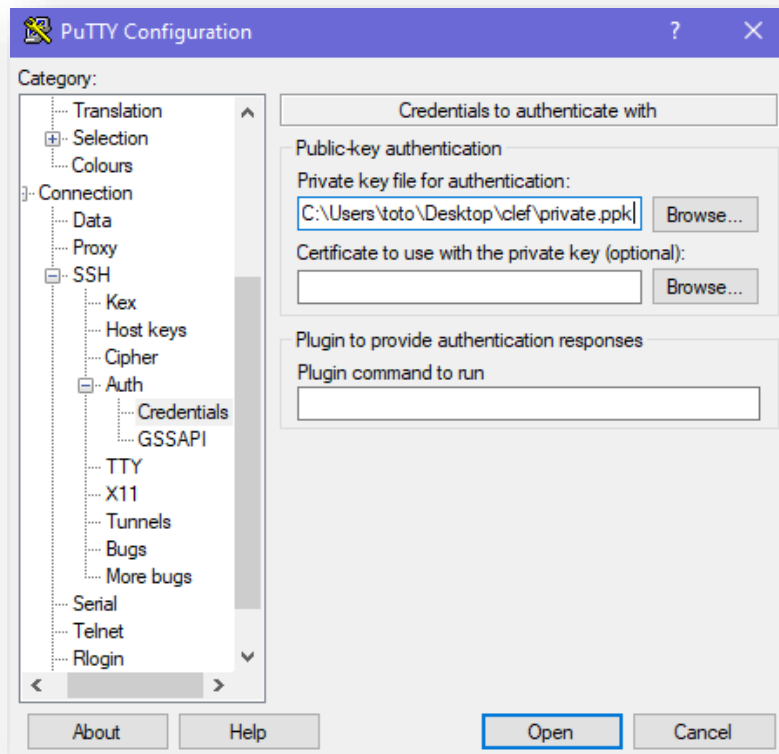
PuTTY est un émulateur de terminal. Il permet de se connecter à des plates-formes Unix (et non-officiellement sur d'autres plates-formes) depuis une machine Windows.

FileZilla est un client FTP, FTPS et SFTP. Il est intégré à la liste des logiciels libres préconisés par l'État français dans le cadre de la modernisation globale de ses systèmes d'informations (S.I.).

2 Contexte

Une **clé privée**, qu'on prendra le soin de protéger par un mot de passe, ne doit pas être partagée et reste uniquement sur le poste à partir duquel on souhaite se connecter.

La **clé publique** est générée à partir de la clé publique, elle est distribuée sur les systèmes auxquels on souhaite se connecter.



3 Téléchargement et installation des outils

PuttyGen est un utilitaire de la suite Putty permettant de générer facilement des clefs RSA permettant de s'authentifier en SSH. Les outils cités dans ce document ne nécessitent pas d'installation sur la machine. Vous pouvez lancer les exécutable directement depuis n'importe quel répertoire.

-> Pour télécharger Putty et PuttyGen : <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>



Package files

You probably want one of these. They include versions of all the PuTTY utilities (except the PuTTY executables) (Not sure whether you want the 32-bit or the 64-bit version? Read the [FAQ entry](#).)

We also publish the latest PuTTY installers for all Windows architectures as a free-of-charge service.

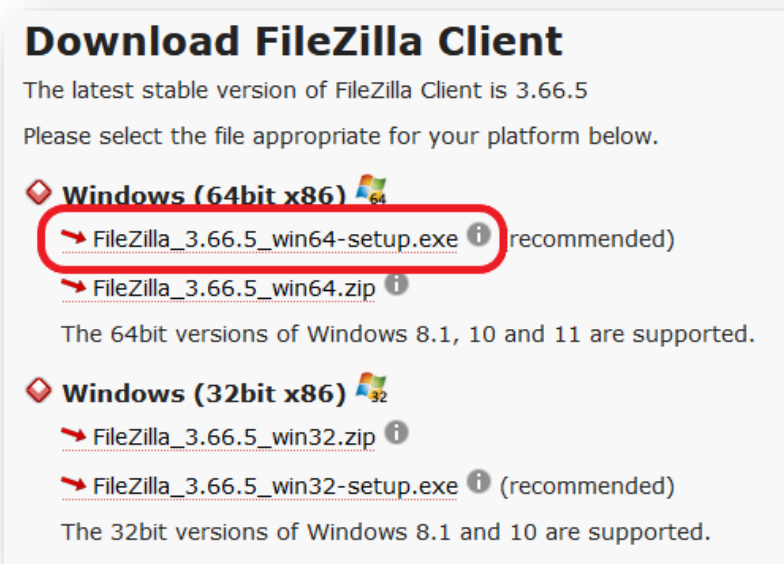
MSI ('Windows Installer')

64-bit x86:	putty-64bit-0.80-installer.msi	(signature)
64-bit Arm:	putty-arm64-0.80-installer.msi	(signature)
32-bit x86:	putty-0.80-installer.msi	(signature)

Unix source archive

.tar.gz:	putty-0.80.tar.gz	(signature)
----------	-----------------------------------	-----------------------------

-> Pour récupérer gratuitement FileZilla : https://filezilla-project.org/download.php?show_all=1



Download FileZilla Client

The latest stable version of FileZilla Client is 3.66.5

Please select the file appropriate for your platform below.

Windows (64bit x86)

- [FileZilla_3.66.5_win64-setup.exe](#) (recommended)
- [FileZilla_3.66.5_win64.zip](#)

The 64bit versions of Windows 8.1, 10 and 11 are supported.

Windows (32bit x86)

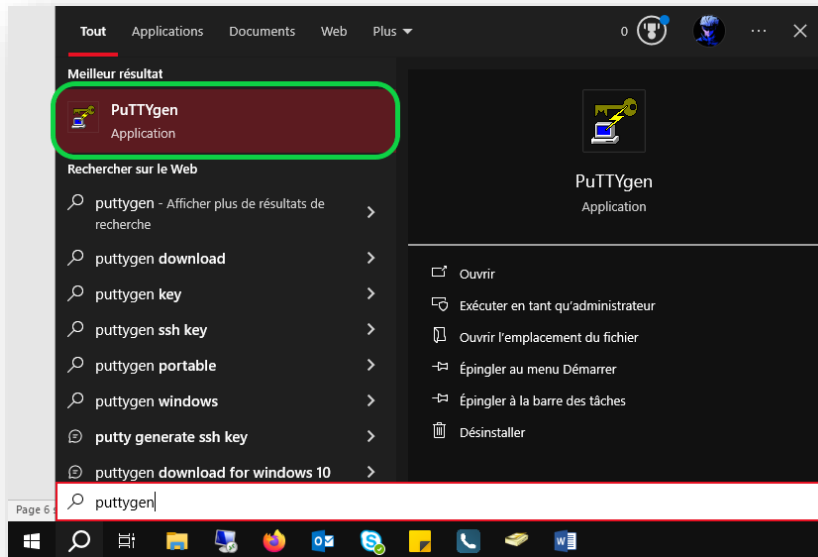
- [FileZilla_3.66.5_win32.zip](#)
- [FileZilla_3.66.5_win32-setup.exe](#) (recommended)

The 32bit versions of Windows 8.1 and 10 are supported.

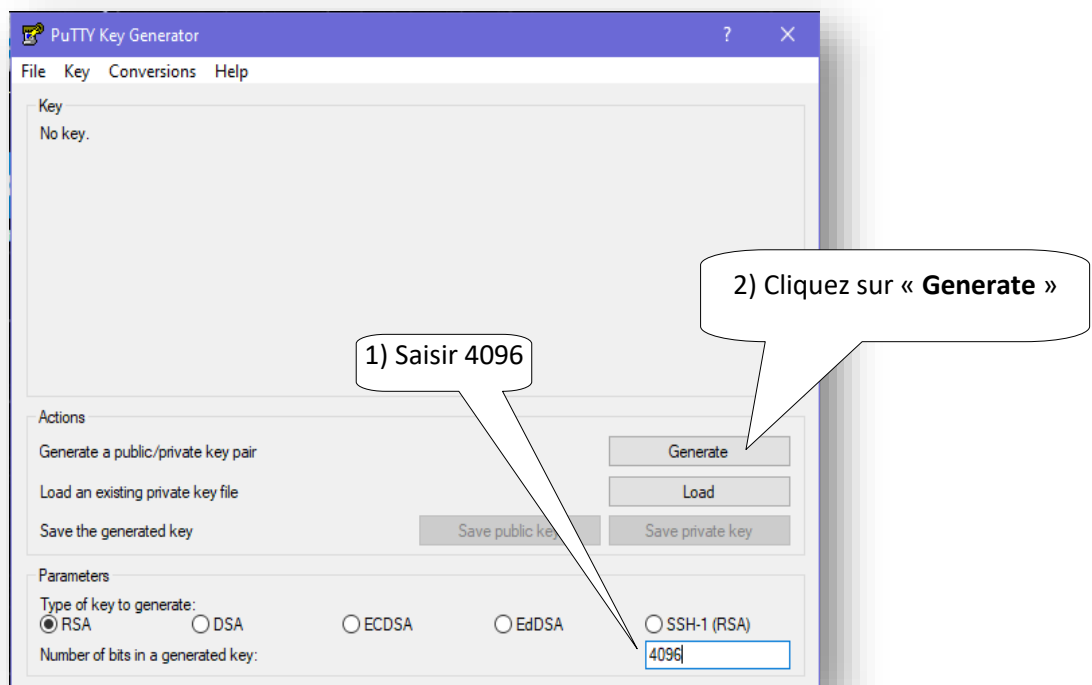
Une fois le Téléchargement terminé, lancez le fichier téléchargé pour installer l'application.

4 Générer des clef RSA

Lancer l'exécutable **puttygen.exe** téléchargé précédemment. Une fenêtre apparaît présentant différents champs et boutons :

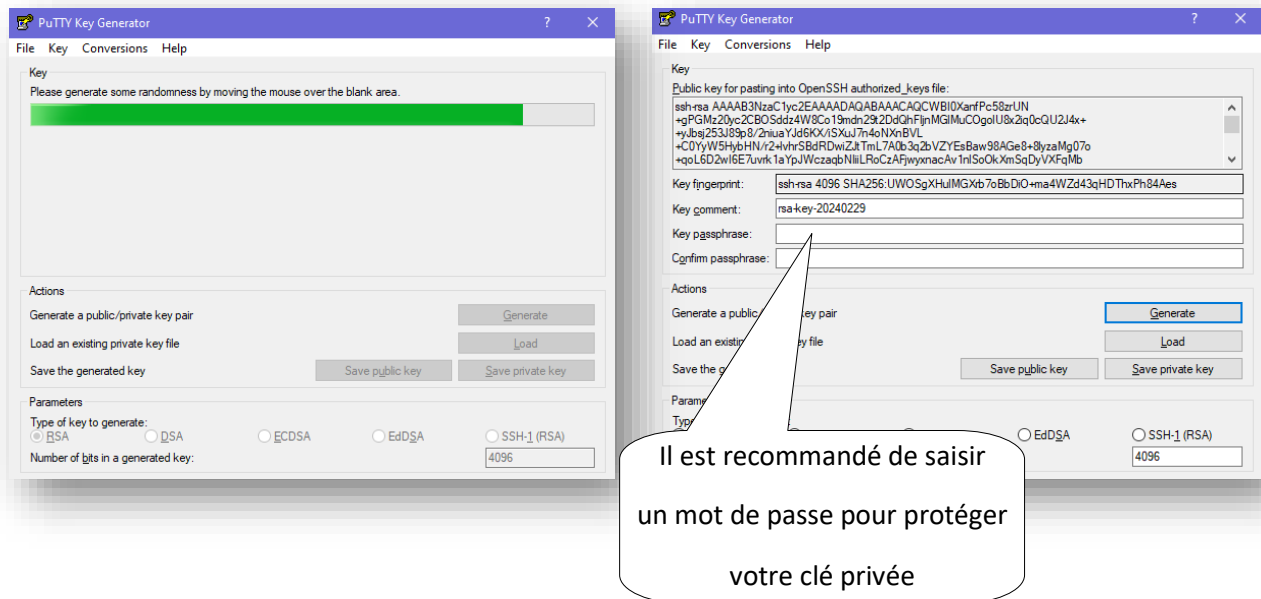


Commencez par saisir la valeur « **4096** » dans le champ en bas à droite puis cliquez sur « **Generate** »



Les boutons se grisent et une barre de progression apparaît dans la zone supérieure de la fenêtre.

NB : Lors de la génération de la clé, il est nécessaire de déplacer le pointeur de la souris sur la fenêtre !!!

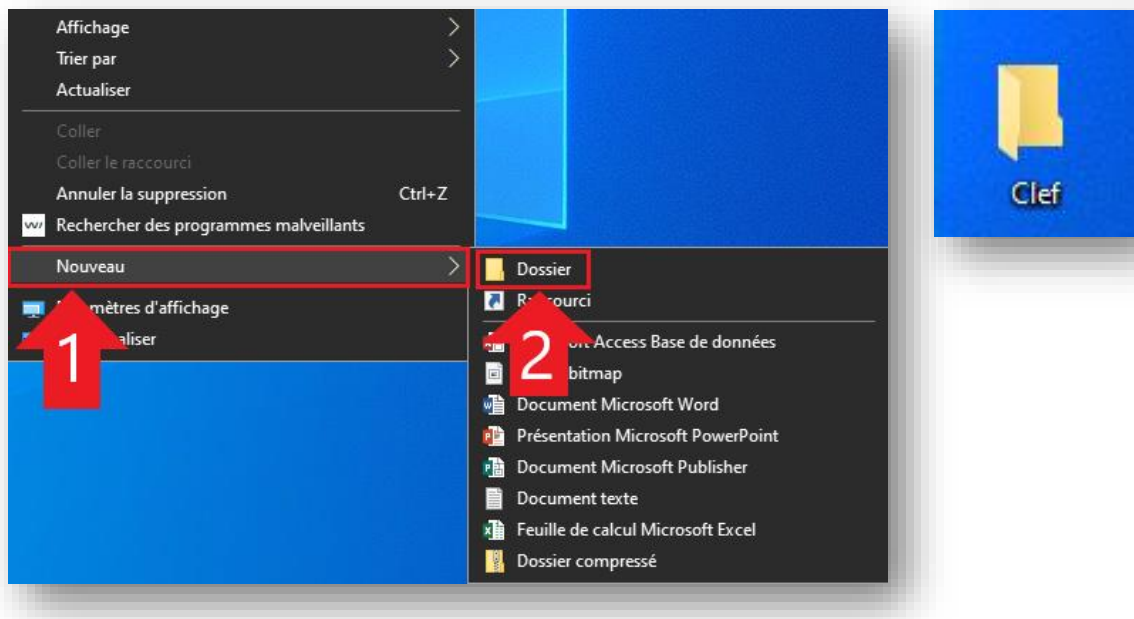


Les clés sont maintenant générées. Il est recommandé de saisir un mot de passe afin de protéger votre clé privée. Ainsi si un utilisateur mal intentionné récupère votre clé privée ne pourra pas s'en servir.

Si vous entrez une « **passphrase** », celle-ci vous sera réclamée à chaque utilisation de la clé (à noter/retenir).

5 Sauvegarde des clefs

Commencez par créer un répertoire « clefs » sur le bureau afin d'y stocker vos clefs.

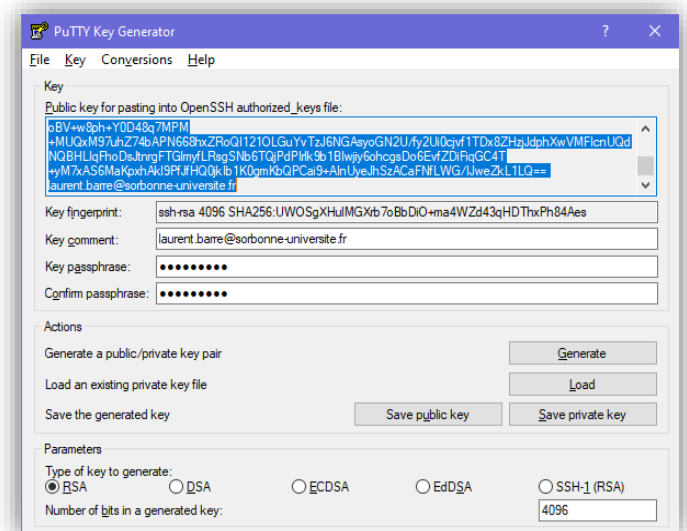


5.1 La clef publique

La zone « *Public key for pasting into OpenSSH authorized_keys file* » en bleue sera utilisée par nos équipes pour déclarer votre clef SSH sur nos plateformes.

Idéalement vous pouvez saisir votre adresse institutionnelle dans le champs « *Key comment* »

- Sélectionnez bien la zone complète de « *ssh-rsa* » du début jusqu'à la fin !
- Copiez le contenu texte (Ctrl+C).
- Ouvrez un éditeur de texte (notepad) et collez-y le texte copié à l'étape précédente (Ctrl+V).
- Enregistrez le fichier dans le dossier « clef », sous le nom **id_rsa.pub**. **C'est ce fichier qu'il faudra fournir à la DSI.**

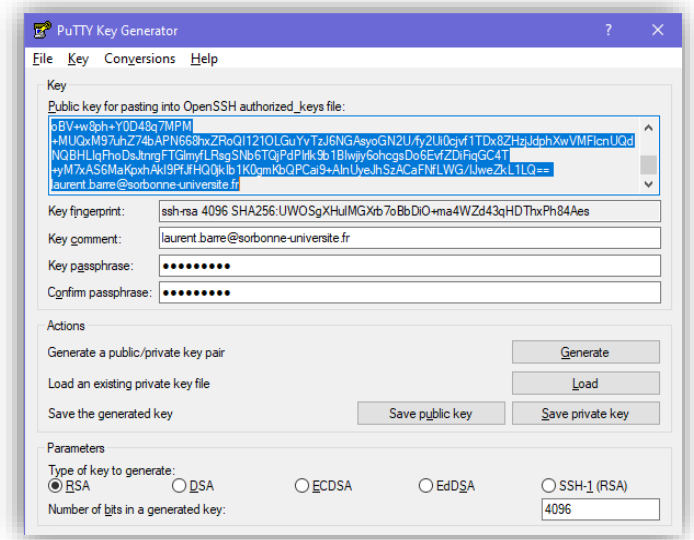


Vous pouvez ensuite cliquer sur « *Save public key* » et enregistrer le fichier dans le dossier « clef » sous le nom **public.key**. (le format est différent mais les données sont les mêmes que dans **id_rsa.pub**)

5.2 La clef privée

Cliquez sur « **Save private key** ». Si vous ne l'avez pas saisi, l'outil demandera confirmation de la sauvegarde de la clef privée sans mot de passe.

Enregistrez la clef privée dans le dossier « clef » sur votre bureau, nommez la « **private** » par exemple.



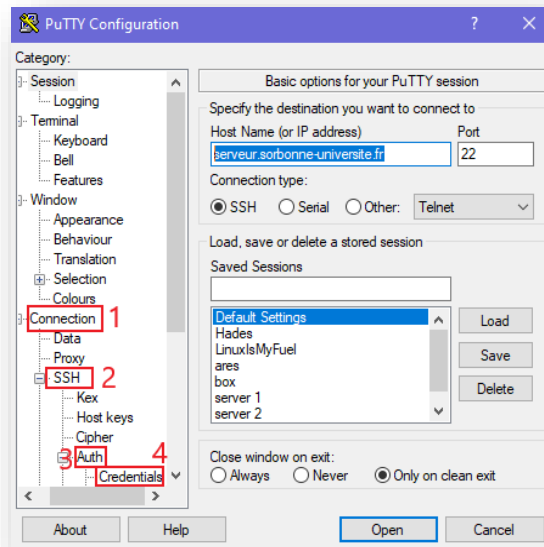
NB : Ne perdez pas ce fichier et le mot de passe associé !!!

6 Ajout de la clef dans Putty

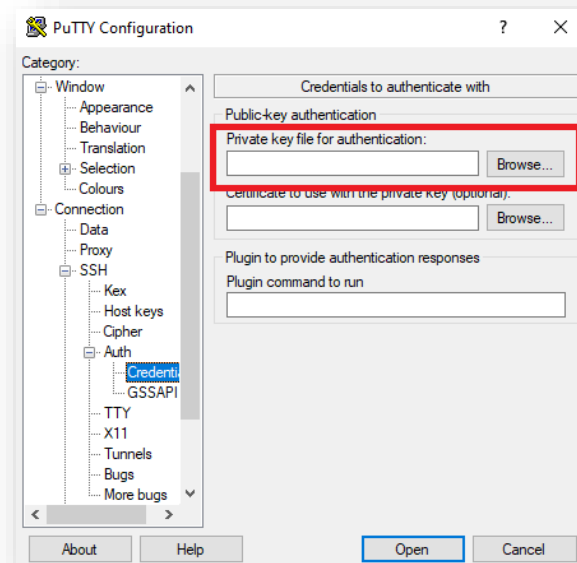
Vous pouvez maintenant tester le fonctionnement de l'authentification par clé SSH. Pour ce faire, fermez PuTTYgen et lancez le client **putty.exe**.



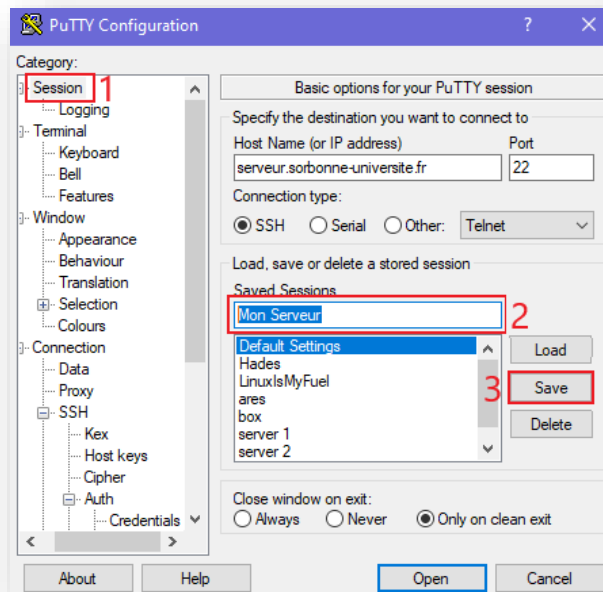
- Sous « **Session** », renseignez le nom de l'hôte ou l'adresse IP du serveur distant correspondant.



- Suivez ce chemin : « Connexion » > « SSH » > « Auth » > « Credentials ».
- Sous « Public-key authentication » (Paramètres d'authentification), puis « Private key file for authentication » (Fichier de clé privée pour l'authentification), cliquez sur « Browse » (Parcourir).



- Cherchez la clé privée « **private.ppk** » dans le répertoire « **clef** » de votre bureau; lorsque vous l'avez trouvée, cliquez sur « **Open** » (Ouvrir).
- Retournez maintenant sous « **Session** » en haut à gauche de la fenêtre et renseignez un nom sous « **Saved Sessions** » (Sessions sauvegardées) puis cliquez sur « **Save** ».



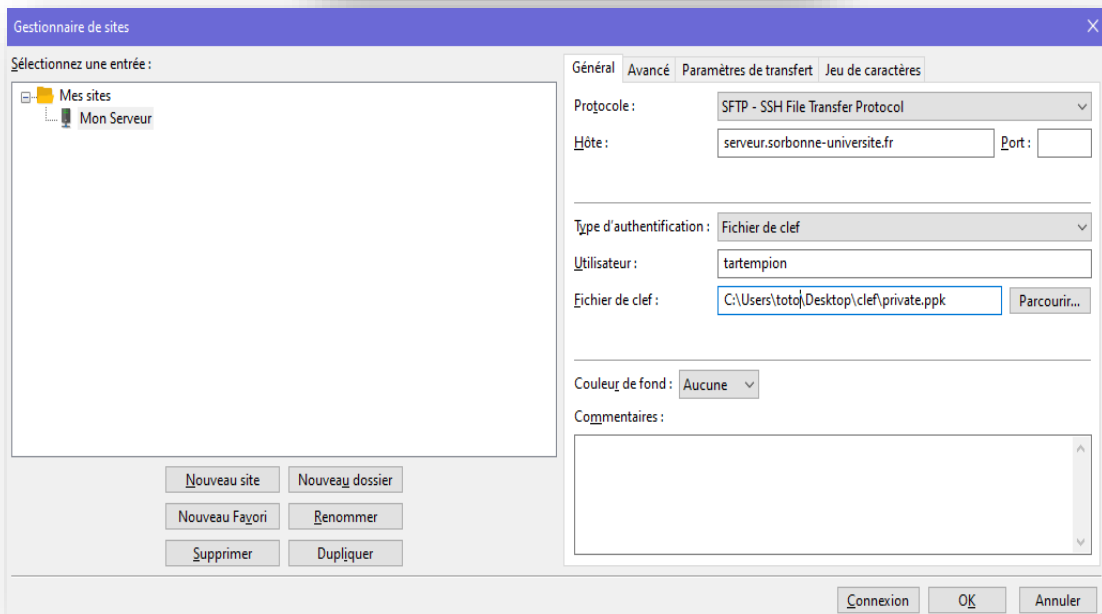
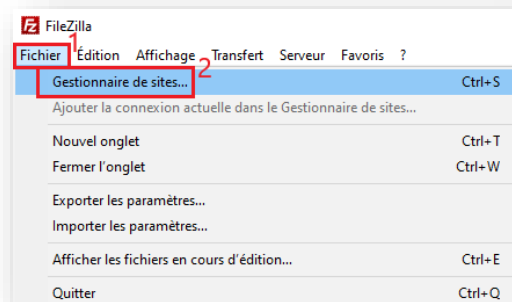
- Cliquez enfin sur « **Open** » en bas à droite de la fenêtre ou double-cliquez sur le nom de la « **Session sauvegardée** » dans la liste pour vous connecter au serveur en utilisant votre clé privée.

7 Ajout de la clef dans FileZilla

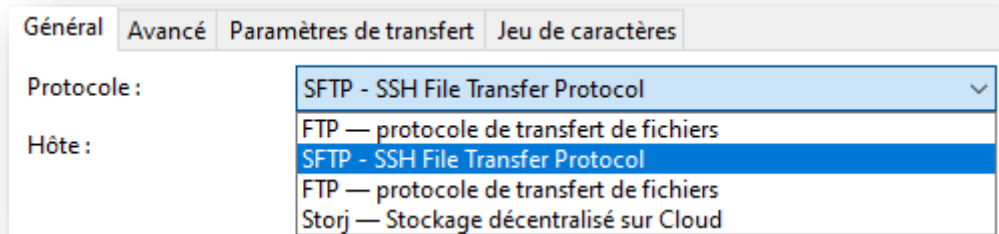
Lancez FileZilla en double-cliquant sur **filezilla.exe**



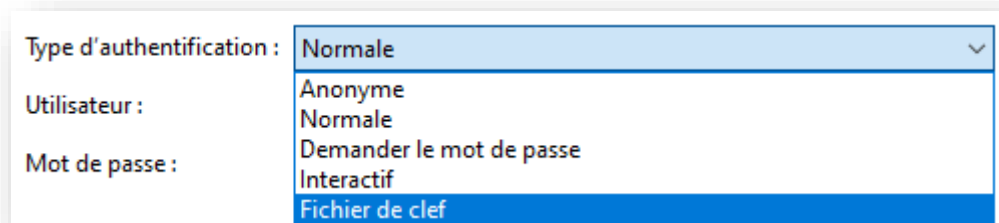
- Ouvrez le gestionnaire de site via le menu « Fichier » > « Gestionnaire de sites » (ou tapez Ctrl+S), une fenêtre s'affiche



- Cliquez sur « Nouveau Site » et donnez un nom à cette connexion (ici « Mon Serveur »)
- Dans « Protocole » choisir « **SFTP – SSH File Transfert Protocol** »



- Dans « Hôte » renseignez le nom de l'hôte ou l'adresse IP du serveur distant correspondant.
- Sur « Type d'authentification » choisir « **Fichier de clef** » puis sélectionnez votre clef privée du répertoire « clef » de votre bureau dans le champ « Fichier de clef »



- Cliquez sur Ok