Manuel des logiciels de transferts de fichiers

File Delivery Services

Editeur

La Poste CH SA
Informatique
Webergutstrasse 12
CH-3030 Berne (Zollikofen)

Contact

La Poste CH SA
Informatique
Webergutstrasse 12
CH-3030 Berne (Zollikofen)
I351 FDS
E-mail : fds@post.ch

Version 5.2 / janvier 2023

Télécharger la version actuelle : https://www.post.ch/fds

Table des matières

1. Généralités

1.1 Introduction

Les utilisateurs FDS peuvent employer le logiciel de transfert de leur choix.

Ce document décrit la création d'une paire de clés SSH ainsi que sa configuration et des conseils pour 2 des logiciels les plus utilisés (WinSCP et FileZilla). Bien que les versions précédentes et ultérieures de ces logiciels ainsi que d'autres logiciels sftp doivent en principe fonctionner sans problème avec FDS, Informatique Poste ne peut offrir qu'une assistance limitée en cas de problèmes.

1.2 Définitions, acronymes et abréviations

Mot	Définition
ssh	SSH (Secure Shell) désigne aussi bien un protocole réseau que les programmes correspondants qui permettent d'établir en toute sécurité une connexion réseau cryptée avec un ordinateur distant.
scp	Secure CoPy ou SCP est un protocole de transfert crypté de données entre deux ordinateurs sur un réseau d'ordinateurs.
sftp	SFTP ou SSH File Transfer Protocol est un perfectionnement du protocole SCP; il permet de transférer des données de manière sûre vers des systèmes distants.
PuTTY	PuTTY est un Client SSH libre, développé par Simon Tatham, pour Microsoft Windows.

2. SFTP

2.1 Introduction

SFTP (Secure File Transfer Protocol) est un protocole sécurisé de transfert de fichiers. Une connexion cryptée est établie entre le logiciel client et le logiciel serveur, rendant ainsi illisibles les données y transitant. SSH garantit l'intégrité et la confidentialité des données échangées.

Attention : SFTP ne doit pas être confondu avec FTPS (FTP via SSL) ou avec FTP via SSH (appelé parfois Secure FTP).

Le serveur SFTP de FDS supporte :

- la version 2 de SSH,
- la version 3 du protocole SFTP,
- les transmissions au moyen du protocole SSH/SCP. A noter que les commandes list, rename et delete ne sont pas supportés par SCP,
- le transfert de fichiers d'une grandeur allant jusqu'à 50 Giga-octets,
- 200 connexions simultanées du même utilisateur,
- blocage automatique de l'utilisateur pendant 30 minutes après 5 connexions erronées successives,
- les formats de clés openSSH, ssh.com et PuTTY,
- la configuration de plusieurs clés SSH par utilisateur.

Le serveur SFTP de FDS ne supporte pas :

- la version 1 de SSH,
- les sessions shell interactives,
- la reprise de transferts interrompus,
- le changement des attributs de fichiers,
- la manipulation de la structure des répertoires.

2.2 Sécurité

Les utilisateurs FDS doivent s'assurer que leur logiciel de transfert de fichiers soit mis à jour. Le fait de n'employer que des algorithmes de cryptage ainsi que des codes d'authentification de message (MAC) considérés comme fiable est particulièrement important.

2.2.1 Algorithmes de cryptage

L'algorithme AES doit être choisi et ceci avec une longueur de clé d'au moins 128 bits.

Le département Informatique de la Poste CH SA se réserve le droit de ne plus supporter des algorithmes dépassés ainsi que ceux n'ayant pas une longueur de clé d'au moins 128 bits et ceci sans préavis.

2.2.2 Codes d'authentification de message (MAC)

Les MAC sont un système de cryptage basé sur des clés symétriques et dont le but est de garantir l'intégrité des messages échangés.

Les MAC fiables sont hmac-sha2-256 ou hmac-sha2-512.

Le département Informatique de la Poste CH SA se réserve le droit de ne plus supporter des méthodes MAC dépassés tel par exemple hmac-sha1 et ceci sans préavis.

2.3 Clé publique et clé privée

La méthode d'authentification la plus simple est par mot de passe. Mais même si celui-ci est crypté, il existe des programmes capables de rompre le cryptage.
Pour cette raison, la seule méthode d'authentification acceptée sur notre serveur FDS est l'utilisation de paires de clés SSH.

Les paires de clés SSH sont des clés asymétriques, ce qui signifie que les deux clés associées ont des fonctions différentes.
La clé publique est utilisée pour crypter des données pouvant être décryptées uniquement avec la clé privée.
La clé publique peut être partager librement, car bien qu'elle permette de crypter des données pour la clé privée, il n'existe aucune méthode capable de déduire la clé privée à partir de la clé publique.

- La clé publique doit nous être communiquée selon les instructions se trouvant dans le « Manuel FDS » et est ensuite enregistrée sur le serveur FDS.

- La clé privée doit toujours rester sur votre ordinateur et ne doit JAMAIS être communiquée !

- La paire de clés doit être générée par l'utilisateur FDS.

- FDS supporte le système de cryptage « RSA » (Rivest-Shamir-Adleman). A noter que « DSA » (Digital Signature Algorithm) n'est plus pris en charge.

- La longueur de la clé doit être d'au moins **4096** bits.

REMARQUE: Afin de protéger la clé privée d'une utilisation non autorisée, il est conseillé de la créer avec un mot de passe (Passphrase). Il faut toutefois observer qu'un mot de passe peut rendre – suivant le logiciel utilisé – une automatisation de la connexion plus difficile à réaliser.

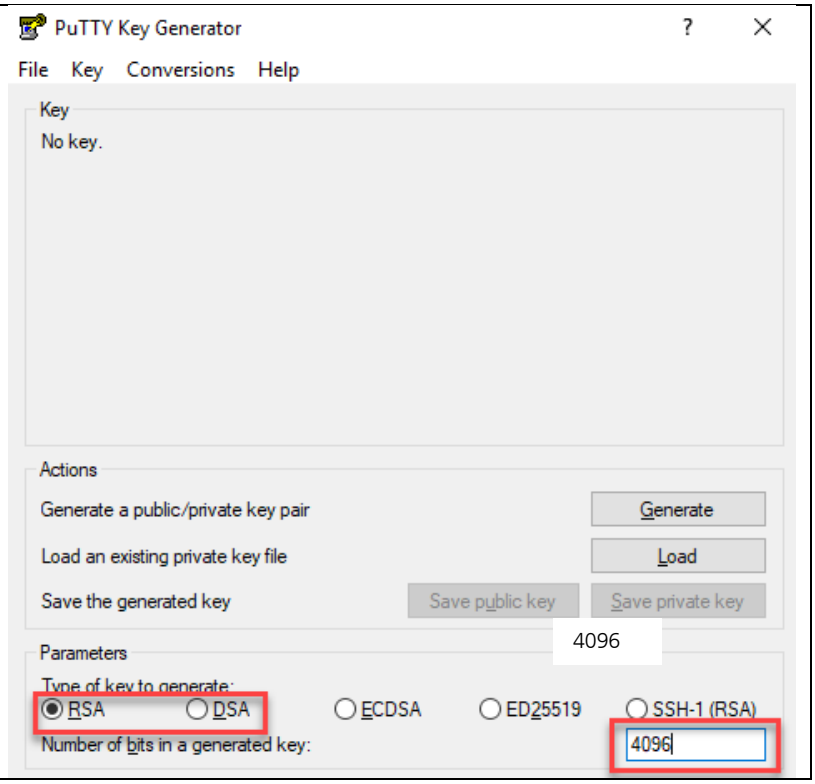
2.3.1 Générer une paire de clés SSH avec PuTTY

PuTTY est un logiciel open source pour Microsoft Windows. Il peut être téléchargé à l'adresse http://www.putty.org

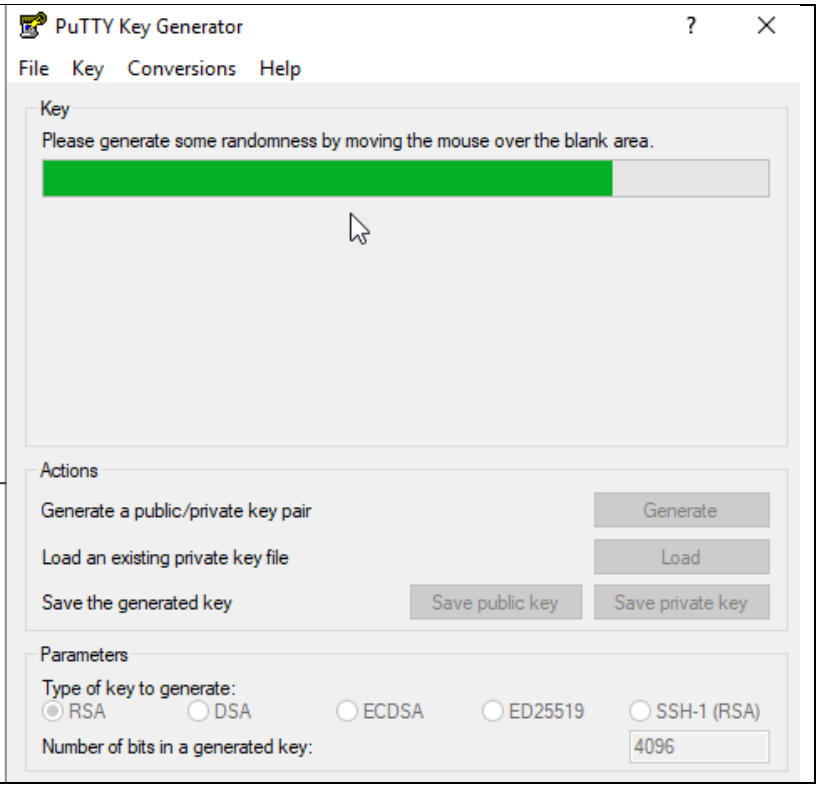
En plus d'un logiciel client SSH/SFTP (putty.exe) il existe la possibilité de générer des paires de clés avec PUTTYGEN

Lancer PUTTYGEN

Vérifier que RSA et au moins 4096 (bits) soient sélectionnés, ensuite: cliquer sur «Generate»

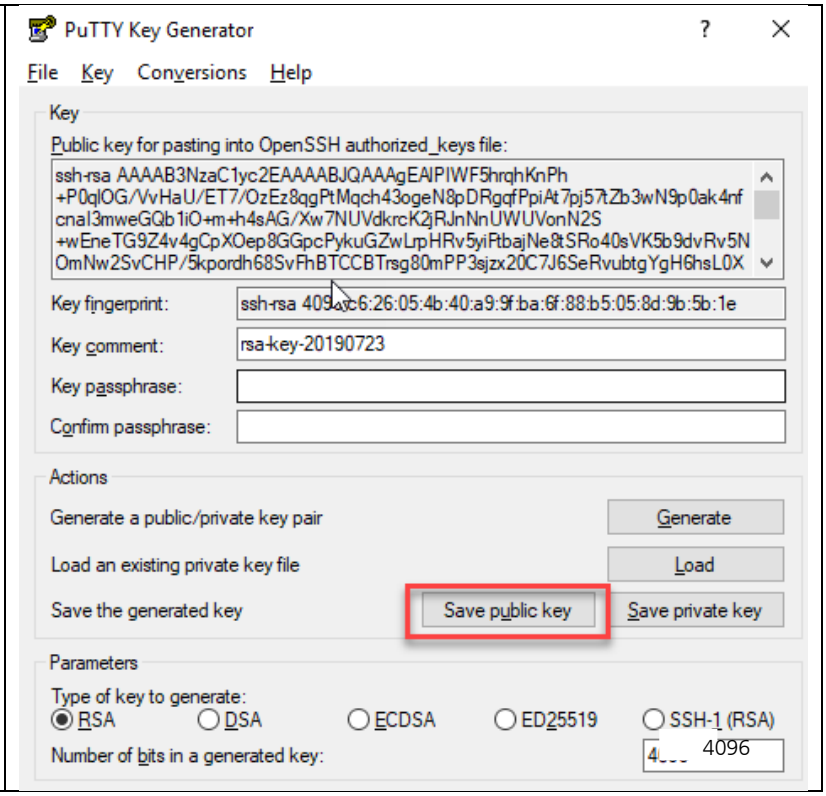


Déplacer le pointeur de la souris sur la surface vide située sous la barre



Lorsque cela est fait, le masque apparaît avec les clés.

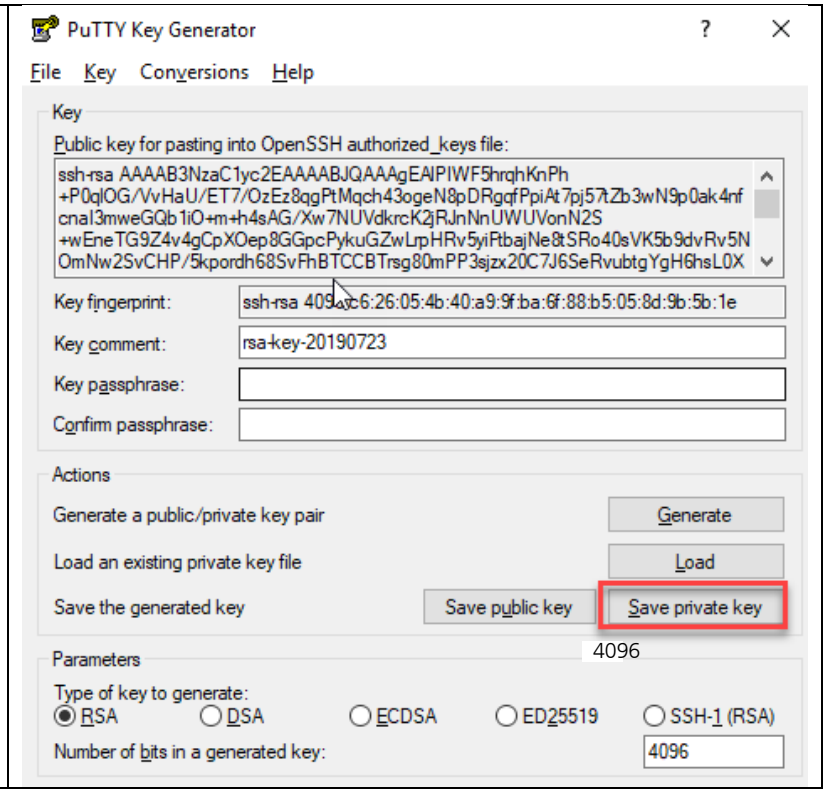
Sélectionner « Save public key »



Sélectionner ensuite «Save private key»

ATTENTION: La clé privée doit toujours rester sur votre ordinateur et ne doit JAMAIS être communiquée!

Afin de protéger la clé privée d'une utilisation non autorisée, il est conseillé de la créer avec un mot de passe (passphrase). Il faut toutefois observer qu'un mot de passe peut rendre – suivant le logiciel utilisé – une automatisation de la connexion plus difficile à réaliser. Pour cet exemple, nous continuons sans passphrase.



2.3.2 Générer une paire de clés SSH avec OpenSSH

OpenSSH est à disposition sur toutes les plateformes Unix. De plus amples informations se trouvent à l'adresse http://www.openssh.com .

La paire de clé peut être générée, par exemple, de la manière suivante :

```
ssh-keygen -b 4096 -t rsa -f /tmp/demo_key -C "commentaire pour la clef demo"
```

Voici un exemple de clé privée:

```
# cat /tmp/demo_key
-----BEGIN RSA PRIVATE KEY-----
MIIJKAIBAAKCAgEAybf8vCaIZc8pSTgpbVUD3aBVC1AnKfBHIqGZA9E7w/TMcs9p
meOU4Nfb9vHqbxPtWlg/qFTG6xRcXhLCjWfE3rV5EQ3sBj3tvLQIZ89Sh/GG21si
< --- SNIP --- >
ACdBLStDxIURm03gmMcBhKHDq4owQlDyESva0LWhIaxFwHpzamOAbPYVqBMbqT38
Bc1eGl0EE4d3yyWoMLOpwbsbhbmjSUjVV4JeDpNciqADBK5mQ3HNGNyKNqQ=
-----END RSA PRIVATE KEY-----
```

Et voici un exemple de clé publique (cette dernière est générée automatiquement avec le suffixe .pub):

```
# cat /tmp/demo_key.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABA < --- SNIP --- > 6mEO5Gh28Vw== commentaire pour la
clef demo
```

3. Connexion à FDS

3.1 Introduction

FDS est atteignable à l'adresse **fdsbc.post.ch** (Internet et lignes louées) ou **fdsbc.pnet.ch** (réseau postal / DMZ de la Poste).

Le serveur SFTP est atteignable sur le port standard 22.

Le nom d'utilisateur ainsi que les détails concernant les noms de répertoires, noms de fichiers, délai de transmission, etc. sont communiqués dans le cadre de la mise en service.

Les fenêtres de maintenance prévues sont publiées à l'adresse https://www.post.ch/fds .

3.2 Test de la connexion

La connexion à FDS peut être testée au moyen de *telnet* :

```
# telnet fdsbc.post.ch 22
Trying fdsbc.post.ch...
Connected to fdsbc.post.ch.
Escape character is '^]'.
SSH-2.0-SFTP Server
```

Attention : deux adresses IP sont utilisées. Ces deux adresses peuvent être déterminées au moyen d'une résolution DNS (nslookup fdsbc.post.ch) en effectuant plusieurs essais jusqu'à ce que la seconde apparaisse. Il ne faut utiliser les adresses IP que pour la configuration des règles des firewalls. Pour la connexion au serveur FDS, il est essentiel d'employer le nom DNS.

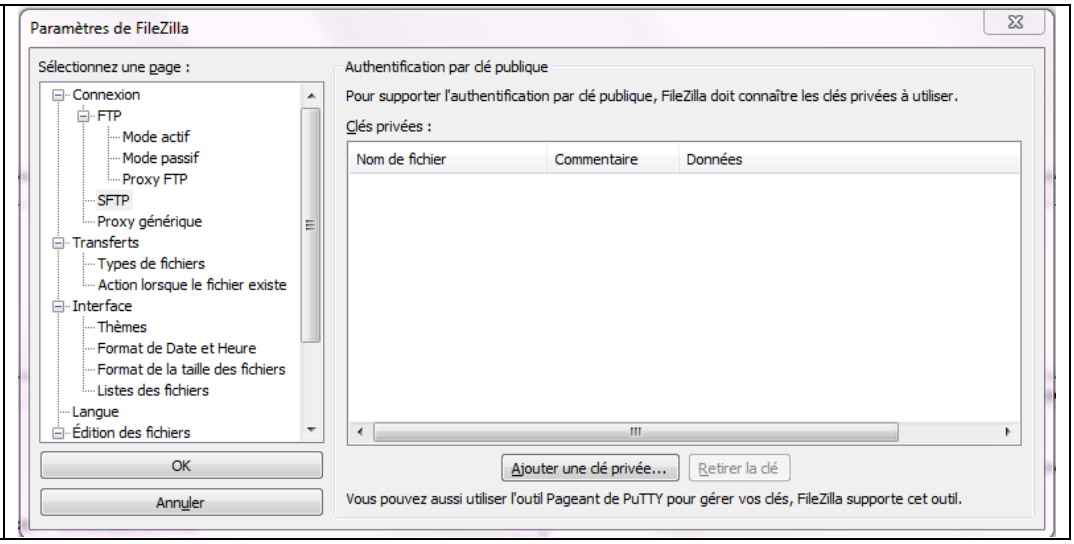
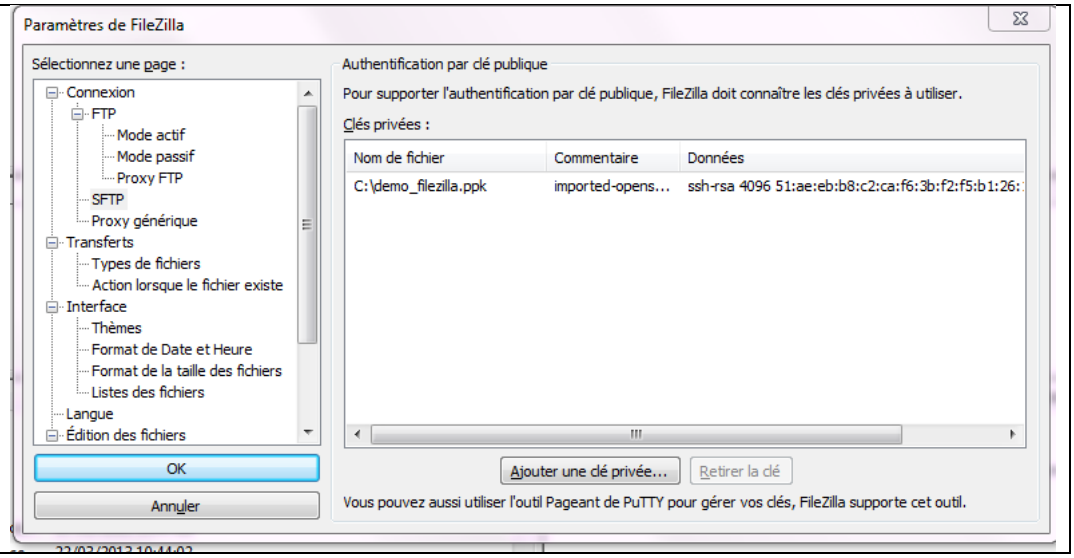
Si vous ne parvenez pas à atteindre le serveur FDS, assurez-vous que votre firewall ne bloque pas la connexion.

Afin que Informatique Poste puisse aider de manière efficace, il est essentiel de communiquer les informations nécessaires (nom d'utilisateur, message d'erreur, heure exacte du problème, noms du fichier et du répertoire).

4. FileZilla

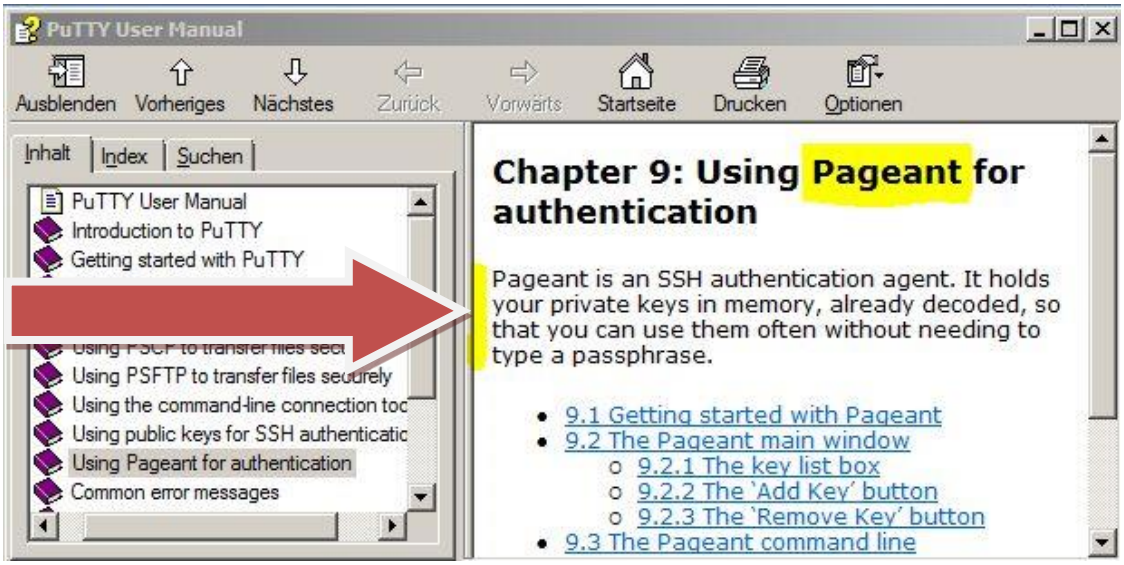
4.1 Importer une clé avec FileZilla

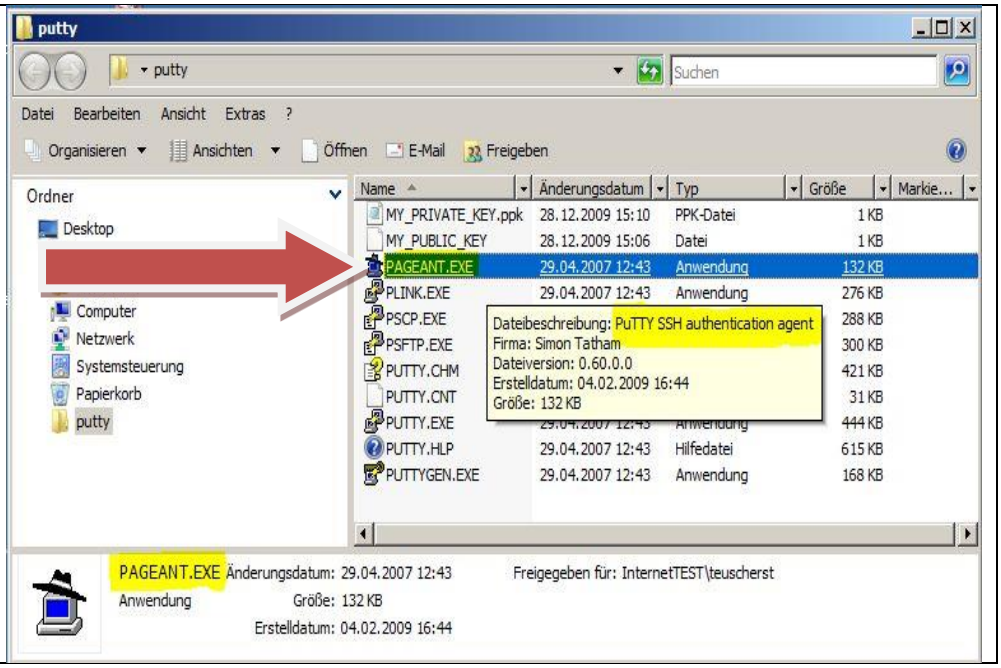
Il est possible d'importer dans FileZilla aussi bien des clés au format PuTTY que OpenSSH.

Lancer FileZilla => Edition => Paramètres … => SFTP => Ajouter une clé privée (puis sélectionner le bon fichier de la clé privée)	
La clé importée est ensuite affiché dans l'écran suivant.	

4.2 Importation automatique avec PuTTY's Pageant

Le «Pageant» (agent d'authentification PuTTY) est un agent SSH qui peut transmettre des authentifications SSH. Pageant peut charger des clés et, sur demande, les mettre à disposition de programmes locaux. L'interface est ouverte, de telle sorte que d'autres programmes peuvent se connecter à ce service de Pageant.

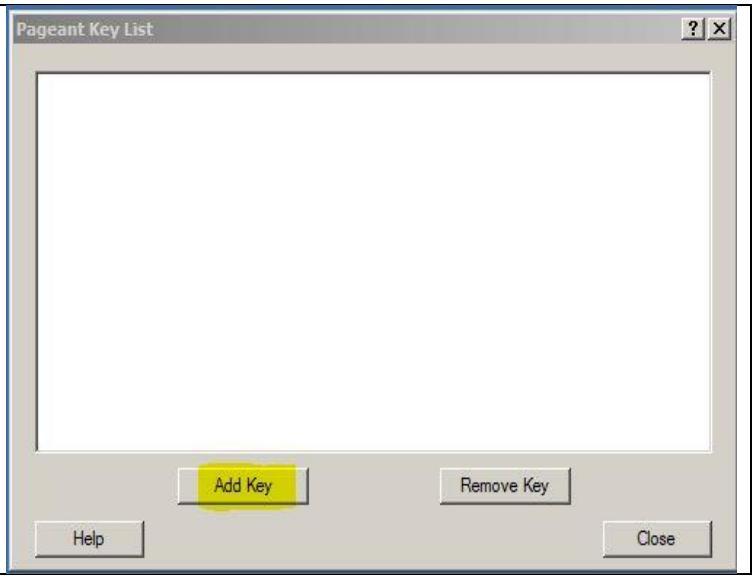


Lancer PAGEANT.EXE	

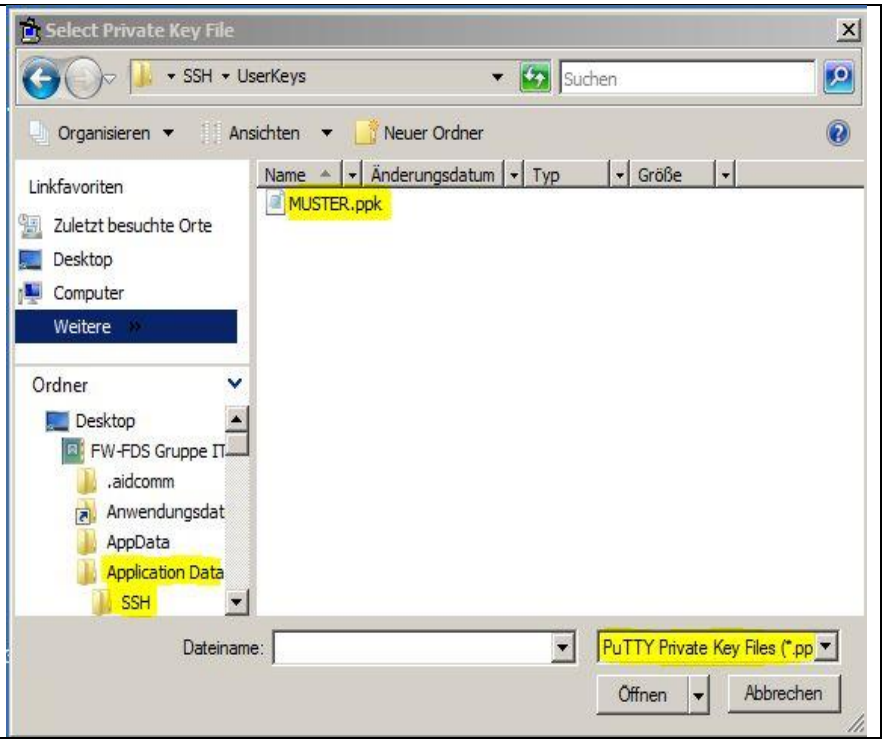
Pageant s'ancre dans la barre des tâches en bas à droite dans la barre de démarrage rapide et indique toutes les sessions enregistrées dans Pageant.

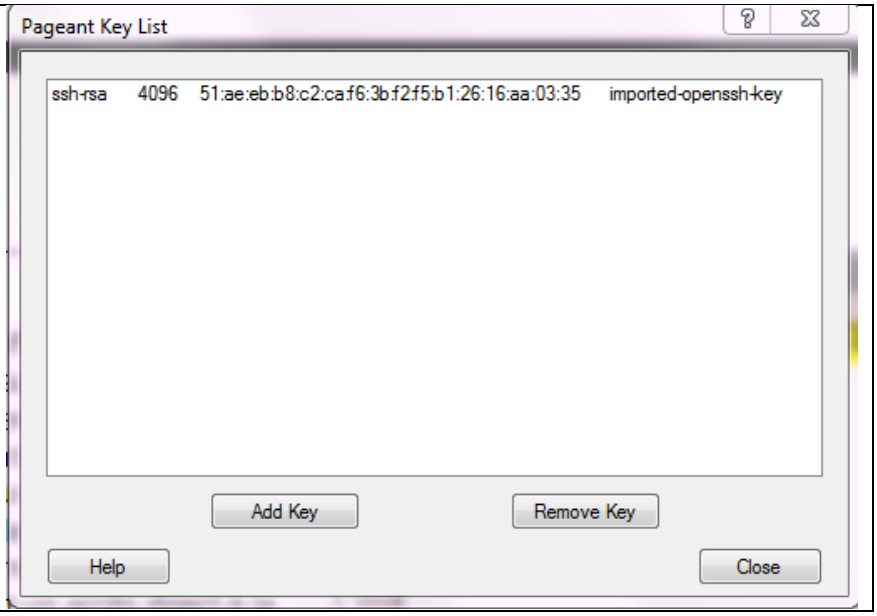
Cette icône apparaît dans la barre des tâches:	

Après l'ouverture, apparaît
la fenêtre (encore) vide «Pageant-Key-List»:

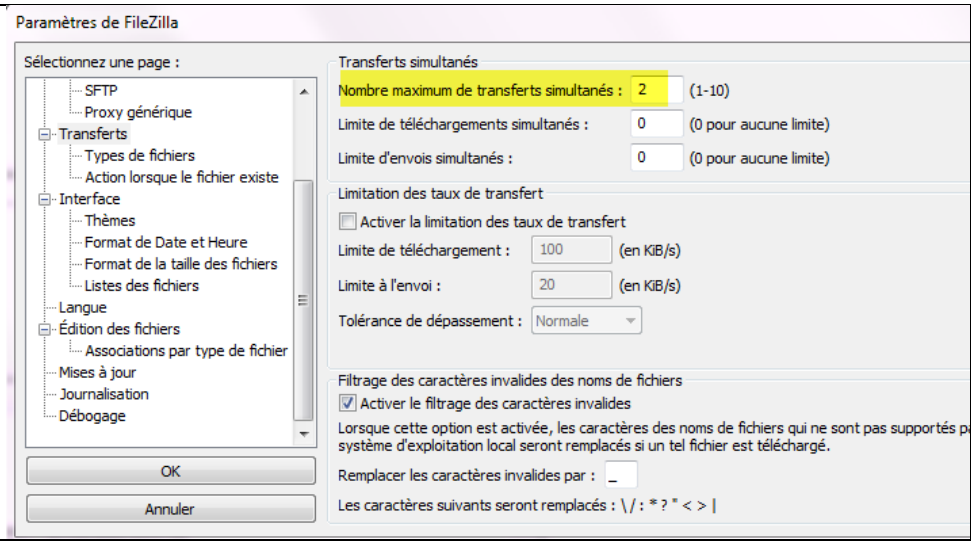


Avec «Add Key», sélectionner la clé privée et confirmer avec «Ouvrir». Ici, seul le format PuTTY est accepté.



Si la clé s'affiche comme l'exemple suivant, elle a été correctement chargée et est maintenant dans la mémoire de l'ordinateur. A partir de la mémoire de l'ordinateur, divers «Programmes SSH» et surtout FileZilla ont un accès direct à la clé.	

4.3 Remarques sur FileZilla

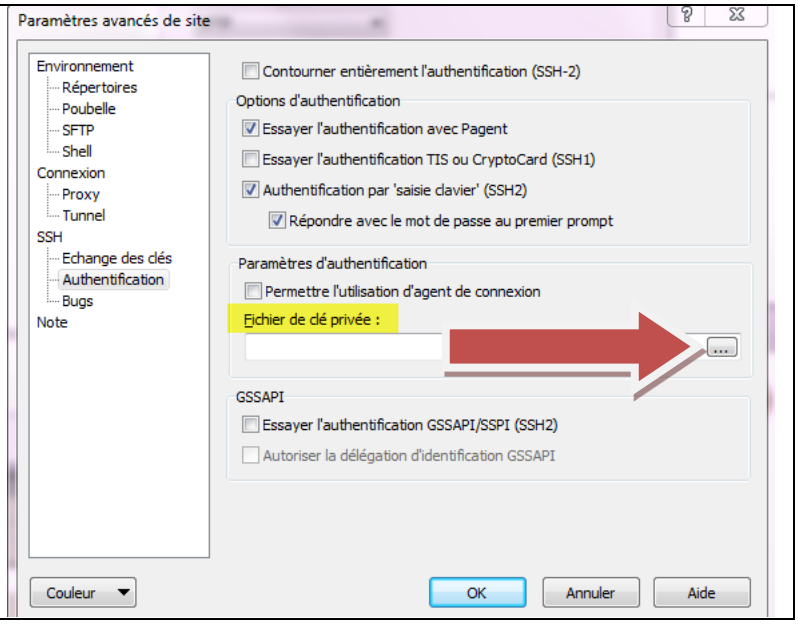
La Poste Suisse a mis en place un système IDS/IPS comme un de ses mécanismes de protection. Afin d'éviter un blocage de l' utilisateur, nous recommandons de limiter le nombre de transmissions simultanées à 3 maximum!	

5. WinSCP

5.1 Importer une clé avec WinSCP:

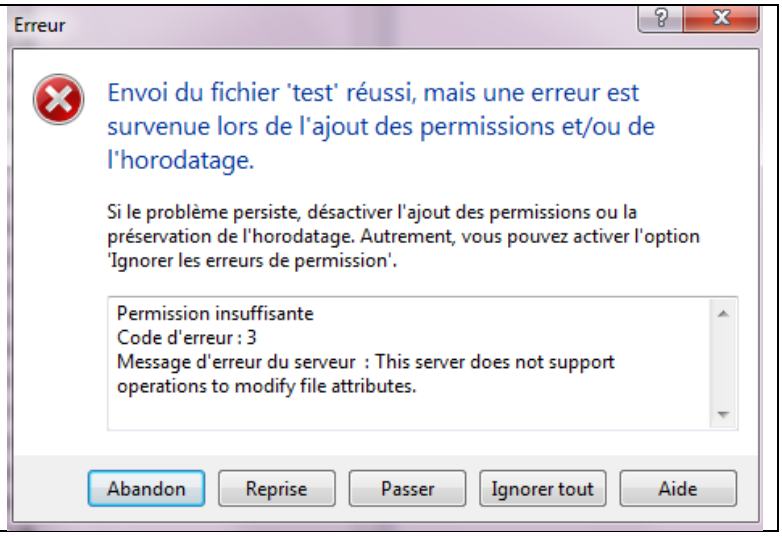
1) démarrer WinSCP
2) cliquer sur « Avancé … »
3) cliquer sur « Authentification »

Cliquer sur le champ « … » et sélectionner la clé privée



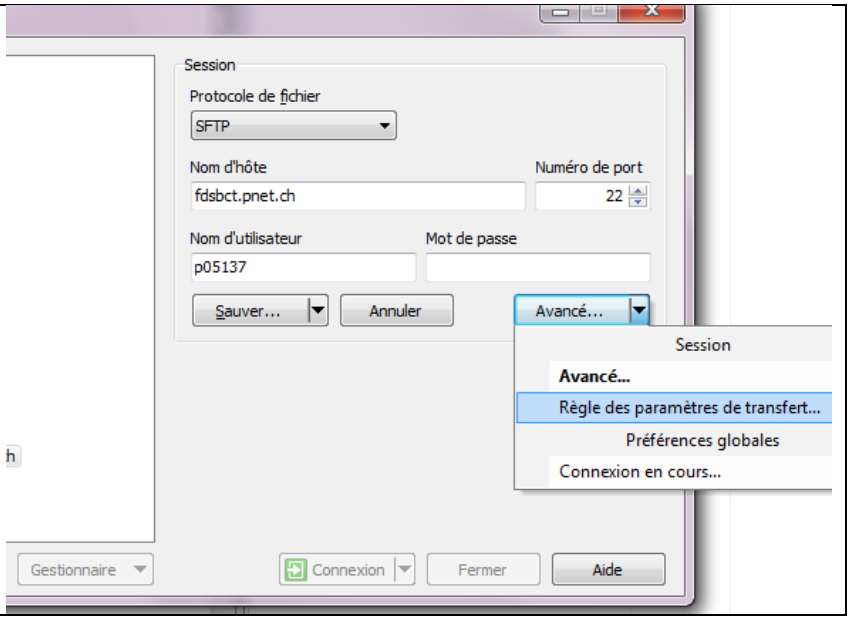
5.2 Remarques sur WinSCP

Si vous avez des problèmes d'autorisation après la transmission des fichiers …



… vous pouvez les corriger sous «Avancé …» …

«Règle des paramètres de transfert …».



=> activez le champ «Ignorer erreurs de permission».