File transfer clients manual

File Delivery Services

Publisher

Post CH Ltd
IT
Webergutstrasse 12
CH-3030 Berne (Zollikofen)

Contact

Post CH Ltd
IT
Webergutstrasse 12
CH-3030 Berne (Zollikofen)
IT17.34 FDS Operation
E-mail: fds@post.ch

Version 5.2 / January 2023

Download the latest version from https://www.post.ch/fds

Table of contents

1. General

1.1 Introduction

The FDS customer may use the file transfer client of their choice.

In this document, the creation of SSH key pair and their configuration as well as important hints for the 2 most used software clients (WinSCP and FileZilla) are described. Although previous and future versions of these software and other SFTP clients as well should generally function without a problem with FDS, our IT unit can only provide limited support for problems or implementation of transfer solutions.

1.2 Definitions, acronyms and abbreviations

Word	Definition
SSH	SSH or Secure Shell refers to both a network protocol and the respective programmes that are used to establish an encrypted connection with a remote computer in a secure manner.
SCP	Secure CoPy or SCP is a protocol for the encrypted transmission of data between two computers in a computer network.
SFTP	SFTP or SSH File Transfer Protocol is a further development of SCP and enables the secure transmission of data to remote systems.
PuTTY	PuTTY is a free SSH client, developed by Simon Tatham for Microsoft Windows.

*

2. SFTP

2.1 Introduction

SFTP (SSH Secure File Transfer Protocol) is a safe file transfer protocol. The connection between client and server is encrypted, making it impossible for an outsider to observe and collect data. SSH assures that data are complete and unchanged from sender to receiver.

Attention: to correct common misconceptions, SFTP is not FTP over SSH (sometimes called Secure FTP), nor is it particularly like FTP at the protocol level. It should also not be confused with FTPS (FTP over SSL).

The FDS SFTP server supports:

- version 2 SSH,
- version 3 SFTP protocol,
- inbound SCP commands using SSH/SCP protocol, as supported by OpenSSH. Note that SCP does not support list, delete or rename,
- transfers of files 50 Gigabytes in size,
- 200 concurrent inbound connections from the same user account,
- user account locking for 30 minutes after 5 failed attempts,
- SSH keys in OpenSSH, ssh.com and PuTTY format,
- more than 1 SSH key for each user account.

The FDS SFTP server does not support:

- version 1 SSH,
- interactive shell session,
- transfer resumption,
- change of file attributes,
- manipulations of the directories structure.

2.2 Security

The FDS customers must ensure that their file transfer software are up-to-date. It is particularly important that only encryption algorithms and message authentication codes (MAC) considered as safe are used.

The Swiss Post and its service and business units will not assume responsibility or liability for any damages that are incurred due to the use of unsecure algorithms and/or MAC methods.

2.2.1 Encryption algorithms

The AES algorithm has to used and with a key length of at least 128 bits.

IT Post reserves the right to not support unsafe algorithms or algorithms with a key length < 128 bits anymore and this without advance notification.

2.2.2 Message Authentication Codes (MAC)

MAC is a symmetric encryption method used to ensure the integrity of a message.

Safe MAC procedures are hmac-sha2-256 or hmac-sha2-512.

IT Post reserves the right to not support unsafe MAC (like as example hmac-sha1) anymore and this without advance notification.

2.3 Public and private key

The simplest authentication method is with password but even though this one will be encrypted, automated scripts can break passwords easily compared to other authentication methods.

For this reason, the only method allowed for authentication on our FDS server is the use of SSH key pairs.

SSH key pairs are asymmetric keys, meaning that the two associated keys serve different functions.
The public key is used to encrypt data that can only be decrypted with the private key.
The public key can be freely shared, because, although it can encrypt for the private key, there is no method of deriving the private key from the public key.

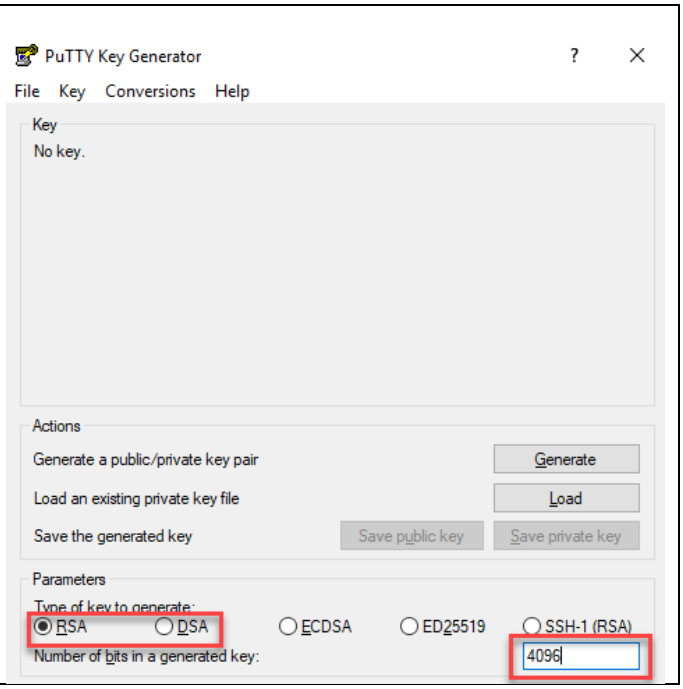
- The public key must be sent to Swiss Post (in accordance with the instructions in the FDS letter of confirmation) and is stored on the Swiss Post FDS server.
- The private key must remain on your computer and may NEVER be given to others!
- The pair of keys must be generated by the participant.
- FDS supports "RSA" (Rivest-Shamir-Adleman) keys algorithm.
- It is required to use a minimum of **4096** bits for the generated key.

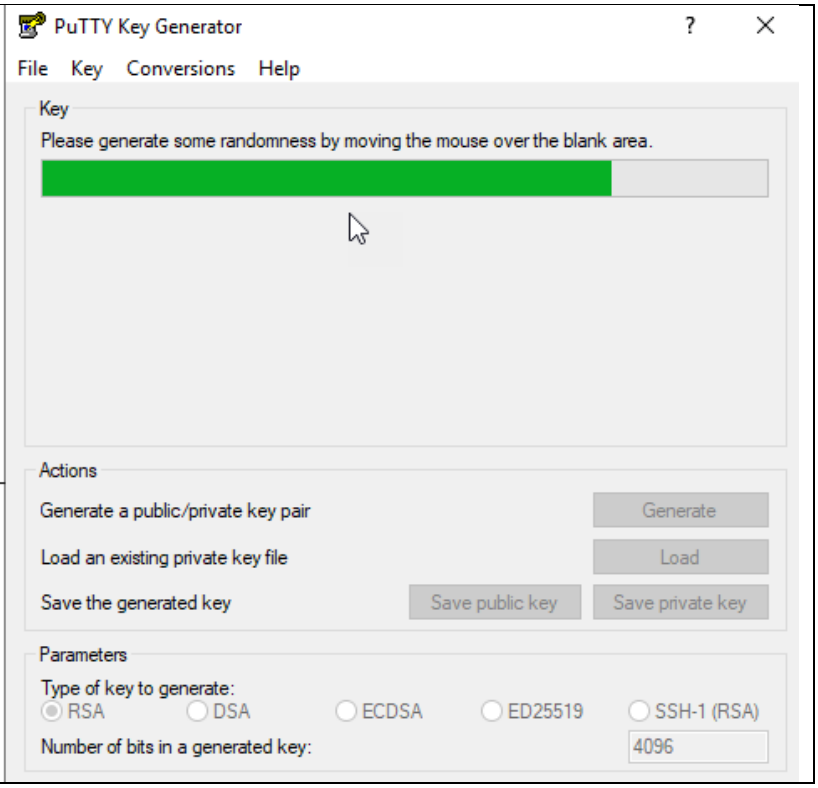
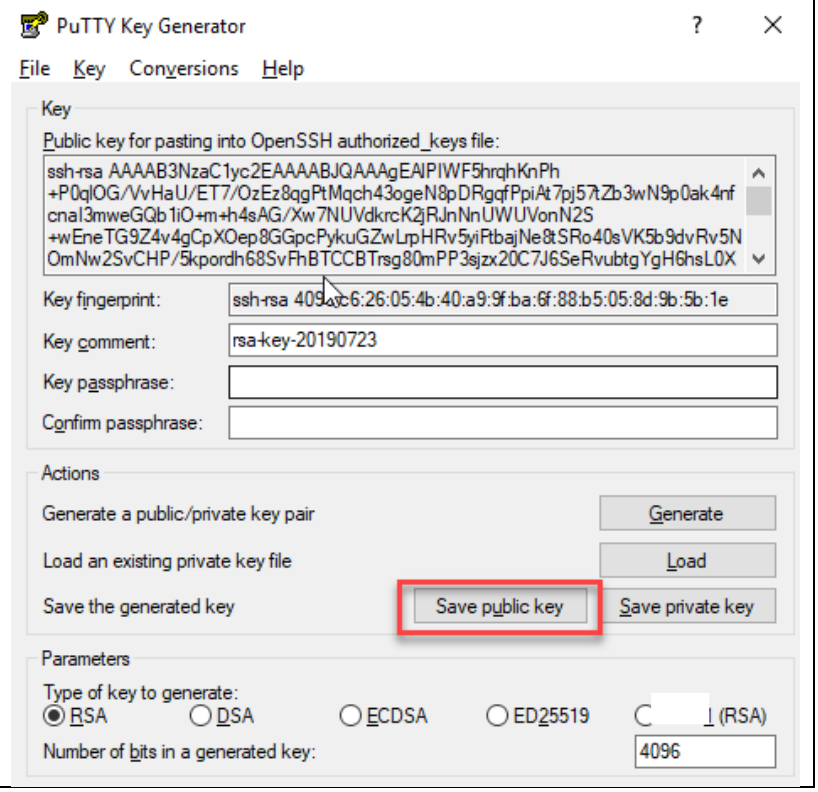
Note: It is highly recommended to protect the key file with a passphrase. This will encrypt the private key when it is saved in a secure location on the local machine. Using passphrases for batch SSH-keys requires familiarity with the SSH-agent authentication subsystem. Participants should be aware that the use of strong encryption methods and encrypted SSH-keys is advisable but will raise administration efforts and system complexity.

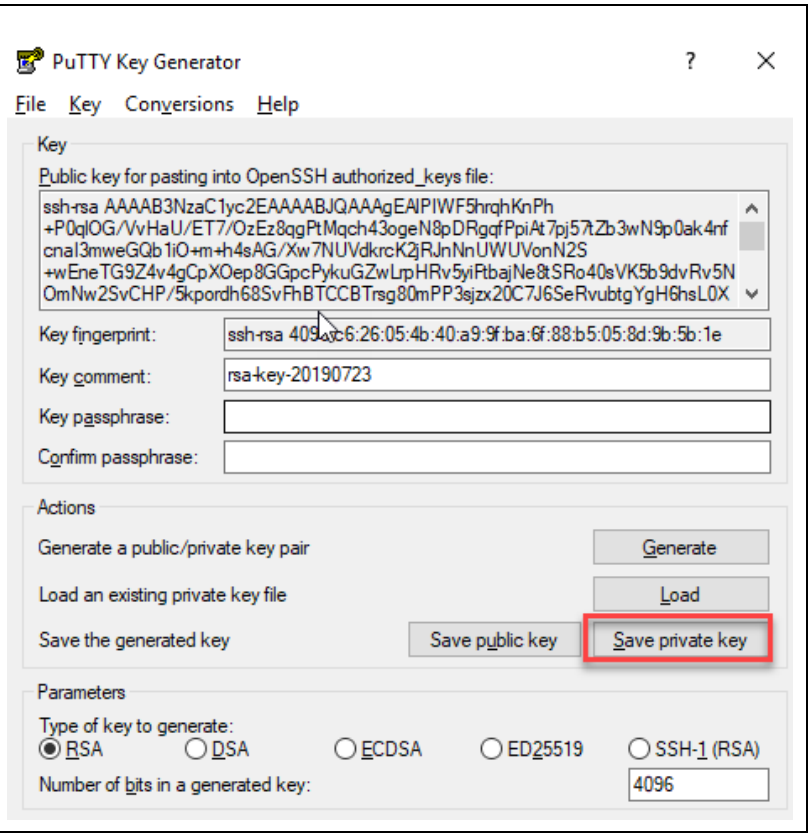
2.3.1 Creating an SSH key pair with PuTTY

PuTTY is an open source software for Microsoft Windows. It can be downloaded at http://www.putty.org .

Beside a SFTP client (putty.exe) puttygen offers the possibility to generate key pairs.

Start PuTTYgen Check whether RSA and at least 4096 (bits) are selected and then: Click "Generate"	

Move the cursor over the blank area	
When it is ready, the mask appears with the keys. Select "Save public key"	

Select then "Save private key" It is highly recommended to protect the key file with a passphrase. This will encrypt the private key when it is saved in a secure location on the local machine. Using passphrases for batch SSH-keys requires familiarity with the SSH-agent authentication subsystem. Participants should be aware that the use of strong encryption methods and encrypted SSH-keys is advisable but will raise administration efforts and system complexity. In this example we will continue without passphrase. PLEASE NOTE: The private key must remain on your computer and may NEVER be given to others!	

2.3.2 Creating an SSH key pair with OpenSSH

OpenSSH is available for any UNIX operating environment and common Linux distributions.
Further information about OpenSSH is available at: http://www.OpenSSH.com

Below is an example of the generation of a key pair using OpenSSH:

```
ssh-keygen -b 4096 -t rsa -f /tmp/demo_key -C "comment for demo key"
```

Here is an example of a private key:

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

And here is an example of a public key (this one is automatically generated with the ending .pub):

```
# cat /tmp/demo_key.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABA < --- SNIP --- > 6mEO5Gh28Vw== comment for demo key
```

3. Connection to FDS

3.1 Introduction

The FDS server is reachable at the address **fdsbc.post.ch** (internet and leased lines) or **fdsbc.pnet.ch** (internal post network).

The FDS SFTP server is running on standard port 22.

Relevant details like username, names of directories, file names, schedule of transmission, etc. are communicated during the service ordering by the respective customer services of the business unit of Post CH Ltd.

Planned service maintenances are published on https://www.post.ch/fds

3.2 Test of the connection

The connection to FDS can be tested using telnet:

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

Please note: the FDS server is using 2 IP addresses. Both addresses can be identified using multiple DNS lookup (nslookup fdsbc.post.ch for instance).
The IP addresses may only be used for the configuration of firewall rules. For the connection from your application to the FDS server, it is essential that you use the domain name.

In case the FDS server is not reachable, please assure that your firewall does not block the connection.

In order to get an efficient help from our side, it is important to provide all needed information (user name, error message, exact time of the concerned connection, file and directory names).

4. FileZilla

4.1 Importing a key with FileZilla

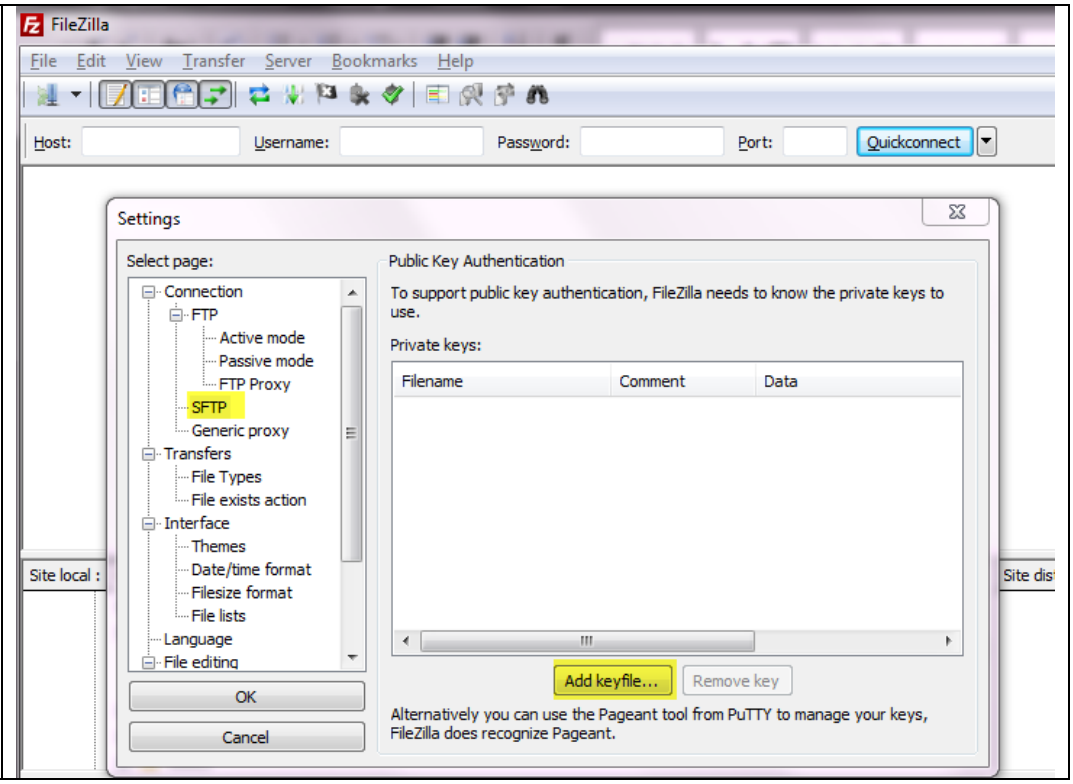
In FileZilla you can import keys in PuTTY format as well as in OpenSSH format.

Start FileZilla

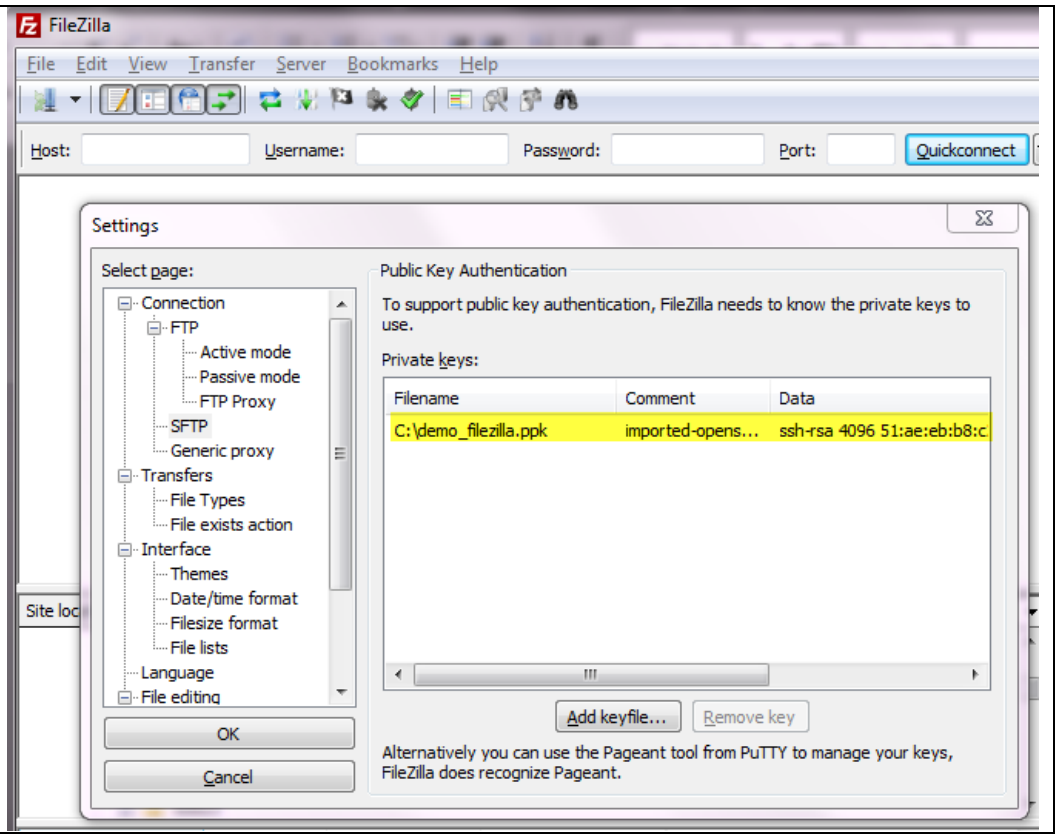
=> Edit
=> Settings
=> SFTP

=> Add keyfile …

(then select the correct private key file)

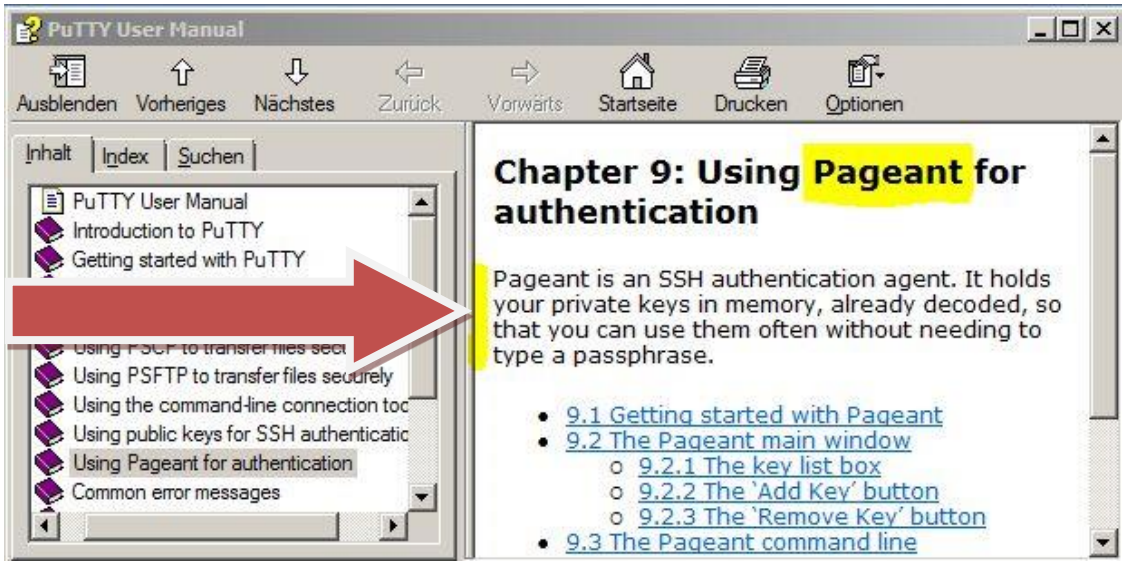


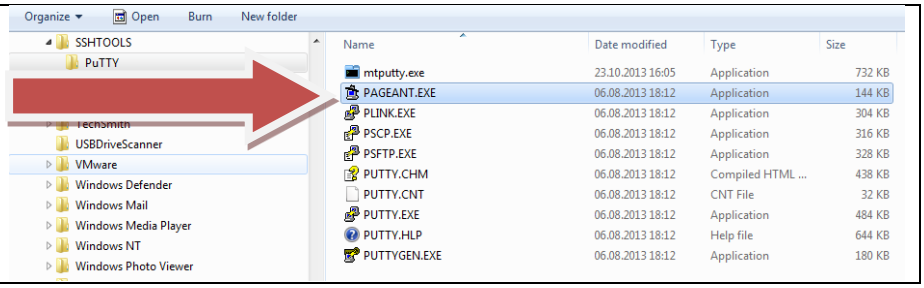
This (yellow) line indicates that the key has been imported successfully.



4.2 Automatic import with PuTTY's Pageant

"Pageant" (PuTTY authentication agent) is an SSH agent which can be used to pass on SSH authentications. Pageant can import keys and make local programmes available when requested. The interface is open, meaning that other programmes can connect up with this service by Pageant.

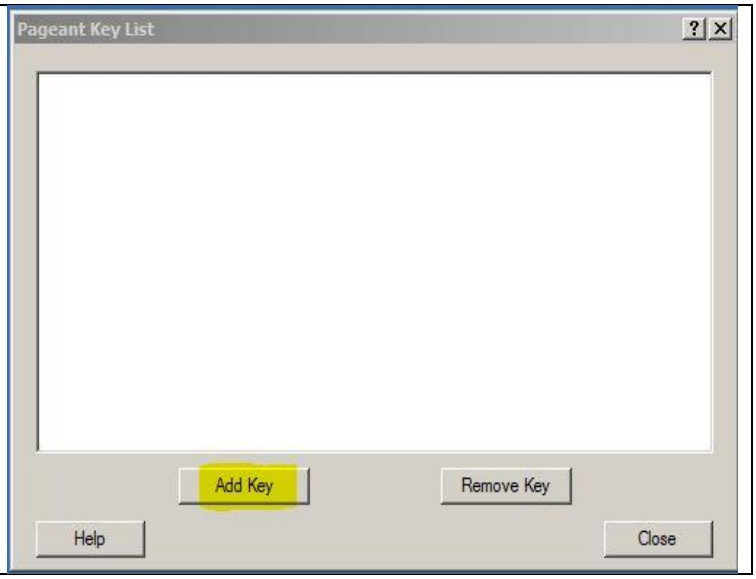


Start PAGEANT.EXE	

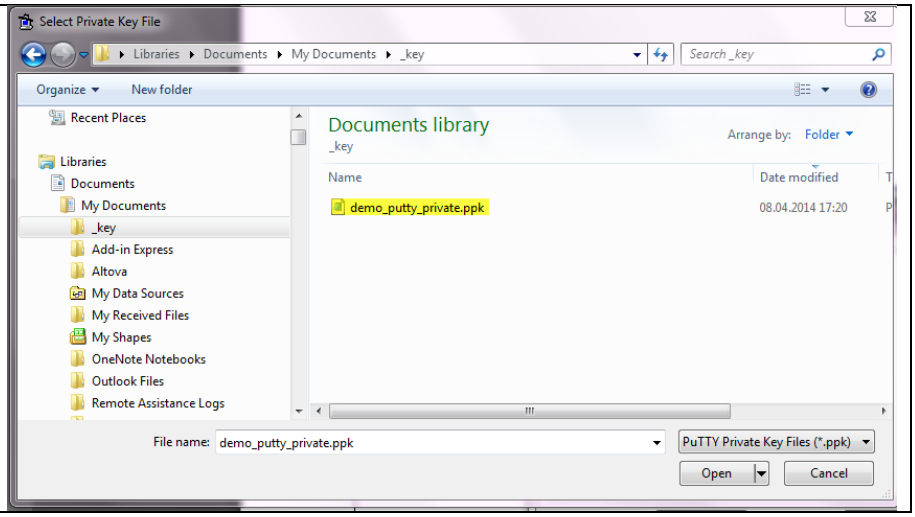
Pageant embeds itself in the System Tray on the right underneath the Quickstart bar and shows all the sessions that are saved in Pageant.

This icon appears in the task bar:	

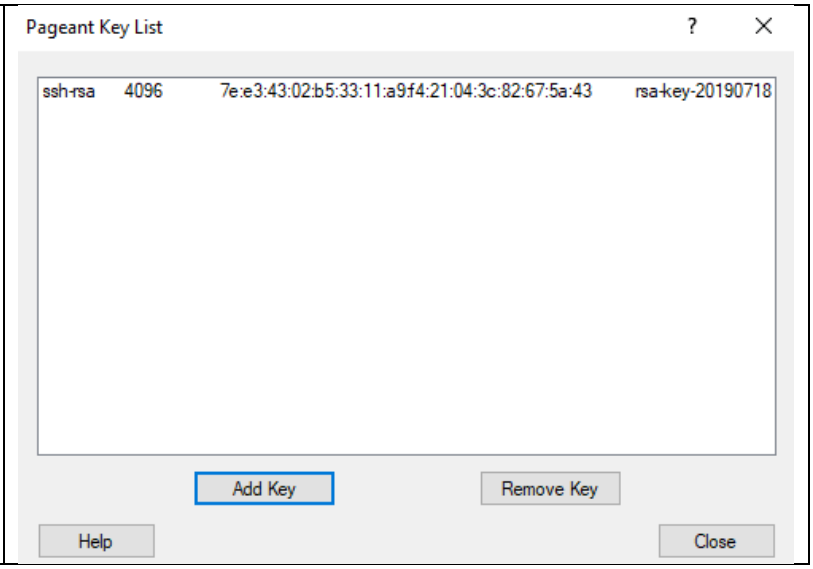
Once it has been opened the "Pageant Key List Window" opens, which at this point is still empty:



Select the private key (*.ppk) via "Add Key" and confirm by clicking "Open". Only keys in PuTTY format will be accepted here.

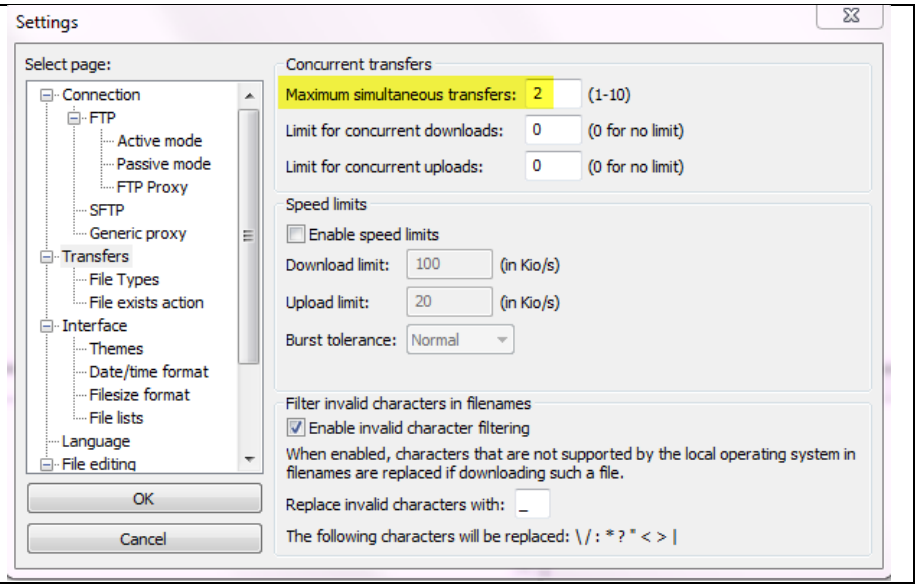


If the key appears as in the following example it has been imported correctly and is now located in the computer's memory. Diverse "SSH programmes" and above all, FileZilla, now have direct access to the key from the memory.



4.3 Notes on FileZilla

Swiss Post also uses an IDS/IPS system as one of its protection mechanisms.
To avoid being locked out, we recommend limiting the number of transmissions taking place at the same time to one or two at the most!

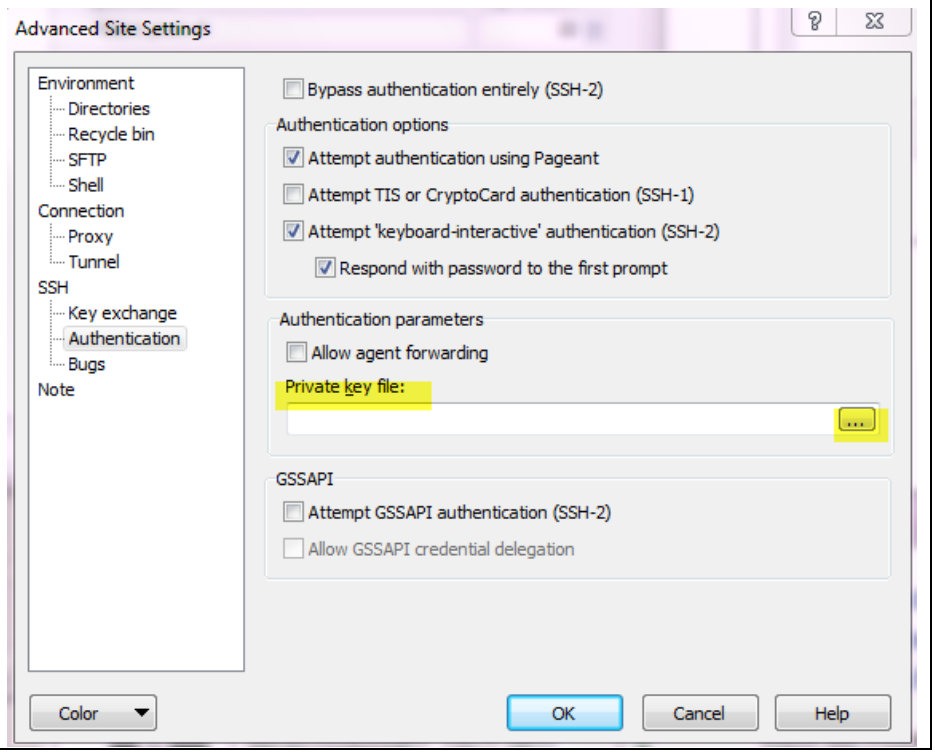


5. WinSCP

5.1 Importing a key with WinSCP

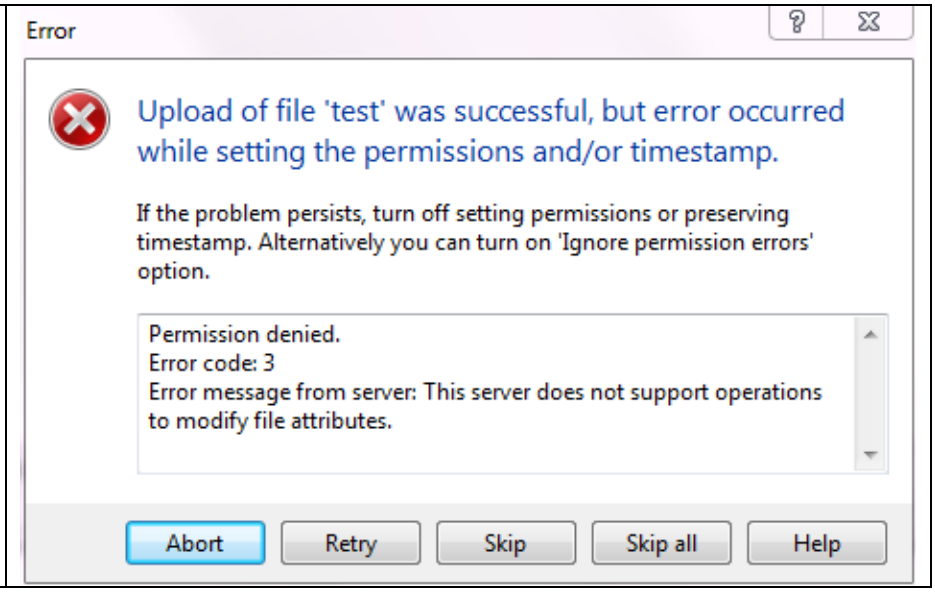
1) Start WinSCP
2) Click "Advanced…"
3) then click on "Authentication"

Click "… –Field" and select the private key



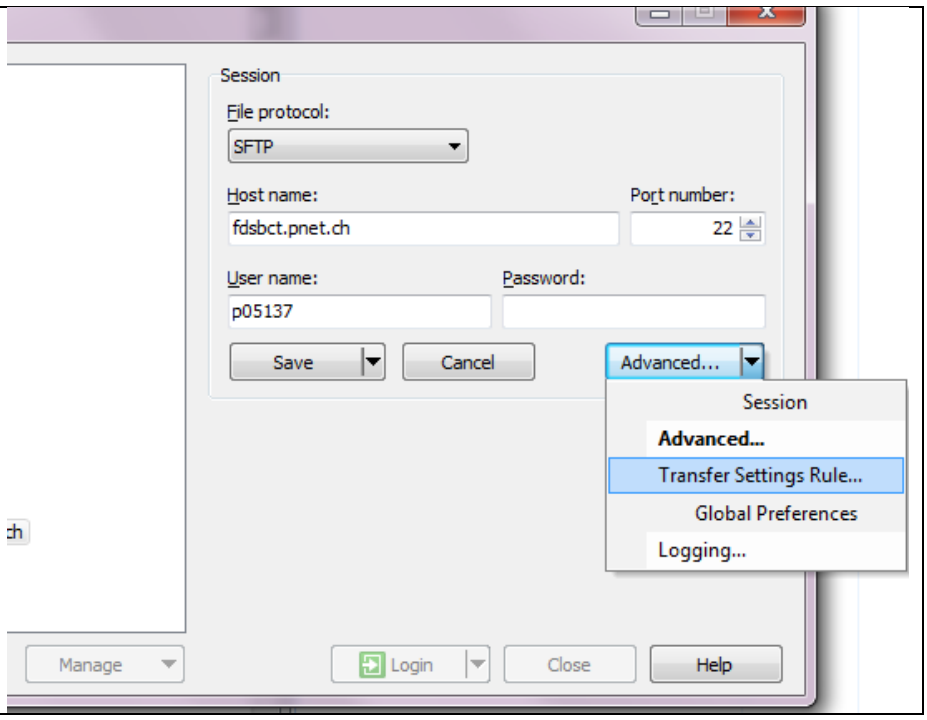
5.2 Notes on WinSCP

If you have problems with permissions after uploading files, this can be rectified by going to …



… "Advanced…" => “Transfer Setting Rule …”

=> Disable the "Set permissions" option and activate the "Ignore permissions errors" fields.



… "Advanced…" => “Transfer Setting Rule …”

=> enable the "Ignore permission error" option.