Managed File Transfer PostFinance (MFTPF) manual

PostFinance

499.81 en (pf.ch/dok.pf) 05.2023

Customer support

If you have any questions about PostFinance products and payment channels, please contact your personal Customer Advisor.

Alternatively, **you can contact our Customer Advice service for business customers:**
Consulting & Sales
Telephone +41 0848 888 900
(max. CHF 0.08/min. in Switzerland)

Publication details
PostFinance Ltd
3030 Bern
Switzerland

Version
May 2023

Contents

1. General information

1.1 Target group for the Managed File Transfer PostFinance (MFTPF) channel

PostFinance Ltd offers its customers various channels for the transfer and collection of data. The Managed File Transfer PostFinance (MFTPF) is a channel for secure and automated data transfer between customers and PostFinance for the efficient handling of payment transactions and the general exchange of data. The service is aimed at business customers who regularly exchange data (payment transaction data, reconciliation files / RAF, software etc.) via a secure channel with PostFinance.

1.2 Using the manual

This manual describes how files are exchanged using the MFTPF server at PostFinance Ltd. It is aimed at those responsible for IT, who establish the connections between the customer's server and the MFTPF server at PostFinance.
The functions of the MFTPF server are described in the first part of the manual. In the second part, you will find the required configuration parameters as well as a description of how to set up the most common SFTP clients and generate the SSH key pair.

1.3 Applicable provisions and manuals

If the Managed File Transfer PostFinance (MFTPF) manual does not include any specific provisions, the General Terms and Conditions of PostFinance Ltd and the Subscriber Conditions for digital services apply. The manual and PostFinance's General Terms and Conditions and Subscriber Conditions can be downloaded at www.postfinance.ch/manuals.

1.4 Registration

Registration to use the MFTPF channel is carried out via your customer advisor or the Customer Center.

1.5 Procedure for using the MFTPF channel

After checking and approving your registration, we will send you your MFTPF User ID.

Besides the MFTPF User ID, you also need an SFTP client and an SSH key pair that you can create yourself.
You are free to choose which client to use. In this manual, we present two of the most common clients (PuTTY and FileZilla) and their connection options.

1.6 Terms and abbreviations

Abbreviation	Definition
DMZ	DMZ stands for demilitarized zone. A DMZ is located on a separate LAN connection of a firewall between an internal network and an unsecured network (e.g. the Internet). Servers that provide services for internet users (e.g. web surfing or email) are frequently set up in the DMZ. In the ideal case, a DMZ lies between two physically separate firewalls. The outer firewall protects against attacks from outside and controls all internet access to the DMZ. The inner firewall controls access from the DMZ to the internal network and vice versa. This means it represents a second line of defence in case the outer firewall is breached. The advantage here is that the internal network is also protected if a hacker manages to reach the web server.
DNS	The Domain Name System (DNS) is one of the most important services on the Internet. Its principal task is the conversion of "internet addresses" into the associated IP addresses.
End-to-end	End-to-end is the connection between an application belonging to PostFinance Ltd and the external customer's application.
FileZilla	FileZilla is an FTP client. It enables the transfer of data via FTP servers – simply using FTP or encrypted using FTPS or SFTP and via SSL or SSH.
FTP	The File Transfer Protocol (FTP) is a network protocol specified in RFC 959 of 1985 for transferring data via TCP/IP networks. It is a protocol that allows files to be exchanged between different computers – regardless of their operating system and location.
GSLB	Global Server Load Balancing (GSLB) primarily serves to distribute access via a central access address to geographically remote data centres. The GSLB technology works along the same general principles as DNS load balancing.
IPSS	LAN Interconnect over IPSS is a service from Swisscom. Swisscom can connect local networks into one single company-wide communications infrastructure. IPSS is Swisscom's own solution using cutting-edge technology. The MPLS (Multi Protocol Label Switching) technology it uses enables great flexibility with regard to bandwidth. The service is provided entirely by Swisscom Enterprise Solution. More information at: http://www.swisscom.com/es/
MAC	MAC (Message Authentication Code) is a cryptosystem based on symmetrical keys; its purpose is to guarantee message integrity.
MFTPF	Managed File Transfer PostFinance (MFTPF) is a service that includes the receiving and sending of files from and to PostFinance.
MPLS	Multi Protocol Label Switching (MPLS) is for implementing label switching. This procedure reduces the burden on the routers involved in transporting a data package as the complexity level is reduced to that of a switch. This is achieved by establishing a fixed connection path at the start of the data transfer. Routers on this path no longer have to search for the recipients of data packages to be forwarded; they simply forward these along the previously established path without further processing.
Public key process	The public key process is an asymmetric cryptosystem that consists of one public and one private key. All users generate their own key pair, which consists of one secret part (private key) and one non-secret part (public key).
PuTTY	PuTTY is a free SSH client for Microsoft Windows.
SCP	SCP is a protocol for the encrypted transfer of data between two computers via a computer network.
SFTP	Secure File Transfer Protocol (SFTP), also known as SSH File Transfer Protocol, is an extension of SCP and allows secure data transfer and data access by a client to remote systems. The protocol does not involve either authentication or encryption. These functions must be undertaken by the underlying SSH protocol. SFTP is not to be confused with Secure FTP or with FTP via SSL.
SSH	Secure Shell (SSH) refers to both a network protocol and the corresponding program that enables the creation of a secure and encrypted network connection with a remote computer.
SSH key pair	A key pair that consists of one secret part (private key) and one non-secret part (public key).
TTL	The Time to Live (TTL) is the validity period given to data in computer networks.
WinSCP	WinSCP is a free SFTP and FTP client software for Windows. WinSCP copies files between local and remote computers using various protocols: FTP, FTPS, SCP, SFTP and WebDAV.

2. Managed File Transfer PostFinance (MFTPF)

2.1 Overview

The Managed File Transfer PostFinance (MFTPF) is the channel for file transfer between PostFinance and its customers and partners. From now on, MFTPF is replacing the FDS product at PostFinance.

2.2 Structure

MFTPF is made up of several application, database and perimeter servers. All components are located in different zones. The file transfer and database servers are in a highly protected zone, to which there is only very restricted access. The file servers, which we call Secure Transport Edge Servers, are externally accessible and are located in less protected zones, to which access is permitted with clients (DMZ). The client/server connections from the external networks always run via the Secure Transport Edge Servers.

MFTPF has a georedundant design. It remains available despite any outage of a data centre.

2.3 Connection

2.3.1 Secure File Transfer Protocol (SFTP)

Only SFTP is used for file transfers between PostFinance and its customers / partners. SFTP is a secure file transfer protocol. It establishes an uninterrupted, encrypted connection between the client and the server, making it impossible for a hacker to read the data and usernames. The public key process is used for authentication. This means that the client can log in to the server without user interaction.
SSH guarantees the complete and unaltered transfer of data from the sender to the recipient.

MFTPF supports SSH-2 (Version 2).

Please note: SFTP is not to be confused with FTPS (FTP via SSL) or with FTP via SSH!

2.3.2 Recommended clients

PostFinance recommends the most common clients WinSCP and FileZilla. Configuration is illustrated in section 4.

2.3.3 Connection types

Files are usually transferred via the Internet.

2.4 Sending and receiving

Different directories for sending and receiving are available to customers on the MFTPF server.
The sending and distribution of a file is event-based. When a file is received, it is forwarded by the MFTPF server to the predetermined destinations. It is not possible to stipulate a specific time for an action to be implemented.

It is possible to send and receive files to/from an external destination system (customer server) through PostFinance. To ensure smooth operation, the following preconditions must be met on the customer side:
– Infrastructure and data centre operational 24/7
– Points of contact for support (telephone numbers, e-mail) reachable 24/7

3. Configuration parameters

The following section gives an overview of the configuration parameters.

3.1 SFTP preconditions

The MFTPF server supports:
- Version 2: SSH Protocol
- Version 3: SFTP Protocol
- Incoming SCP instructions with SSH/SCP protocol (Please note: SCP does not support the instructions *list, rename* and *delete*.)
- Encryption algorithms: AES with key lengths of at least 128 bits
- Message Authentication Codes (MAC): hmac-sha2-256
- Transfers of files of up to 50 gigabytes
- 50 simultaneous connections from the same account
- Locking the account after 3 failed login attempts
- Keys in the formats OpenSSH, ssh.com and PuTTY are supported
- One or several keys can be configured per account

3.2 Host name, port and IP addresses

Environment	Host name	Port
Production	mftp1.postfinance.ch	8022

The distribution of communications over two locations is accomplished using DNS load balancing (round robin). This means that the IP addresses of both locations are returned alternately.

It must be ensured that communication to or from MFTPF is permitted in your network. In many cases, the network team has to allow connections with the appropriate firewall rules. Two IP addresses are used. These IP addresses may be used only for configuring firewall rules. The DNS name must be used to make the connections.

Both IP addresses can be determined with several DNS resolution lookup requests (nslookup mftp1.postfinance.ch).
MFTPF supports IPv4 and IPv6. Use of IPv6 requires continuous IPv6 support in your infrastructure.

3.3 DNS caching

The platform operates in active/active mode at two locations. The failover mechanism is guaranteed by a *Global Server Load Balancing (GSLB)* infrastructure. In order to benefit from a rapid failover of the connection to MFTPF, you must ensure that no additional DNS caching is undertaken in your environment. The Time to Live (TTL) specification given by PostFinance's DNS must be respected.

3.4 Authorization

The username (MFTPF User ID) and a valid SSH key pair are needed for connection to the MFTPF server.

Usernames (MFTPF User ID)
The username is communicated during the ordering of the MFTPF channel.

Public key
The SSH key must be at least 4096 bits long. The cryptosystem is RSA.

There is also the option of configuring several public keys for the same usernames. Likewise, several users can use the same key.

PostFinance must also be sent a copy of the public key as per the registration.

3.5 Directories

The directories are created by PostFinance. Users cannot create or delete directories.

The directory syntax includes the following characters:
– Characters: [a–z], [0–9], [. -] (full stop, hyphen)
– Start: The first character must be [a–z], [0–9]

We tell you about the directories relevant to you during registration of the channel.

3.6 File names

The following characters can be used for file names:
– Characters: [A–Z], [a–z], [0–9], [. - _] (full stop, hyphen, underscore)

The file names issued by PostFinance differ according to service but they follow the syntax described above.
Please note that files you create must adhere to this syntax. This is the only way we can guarantee that the files are processed.

4. Creating the SSH keys and setting up the client

This section illustrates how to generate the SSH keys with PuTTY and OpenSSH and how to configure the most common clients FileZilla and WinSCP for file transfer.

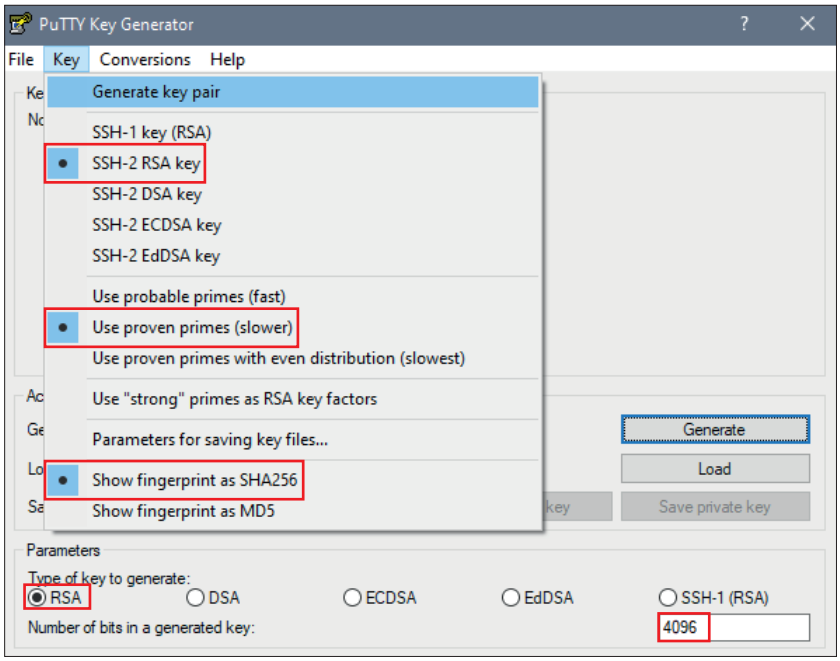
4.1 Creating an SSH key pair with PuTTY

PuTTY is open source software for Microsoft Windows. It can be downloaded from http://www.putty.org.
The private and public key can be generated separately with the SSH/SFTP client (putty.exe). PuTTYgen offers the option to generate key pairs.

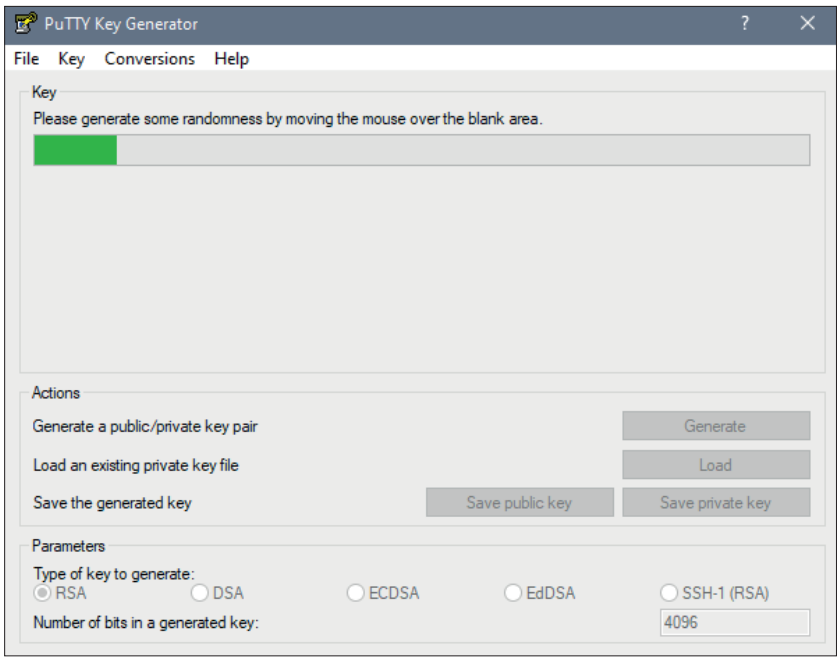
Start PuTTYgen.

Select *SSH-2 RSA* as key type.
Enter *4096* bits as length.

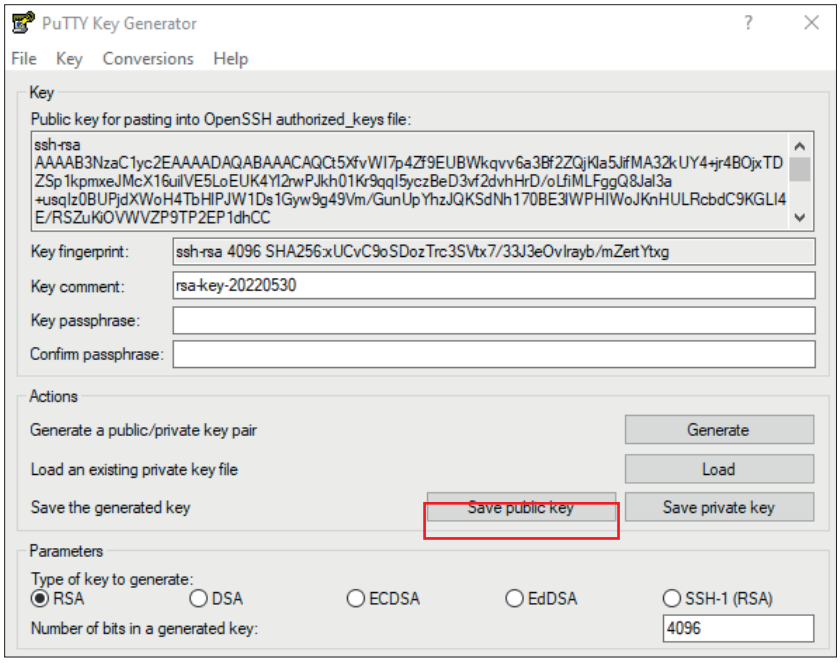
Click *Generate*.



Move the mouse pointer over the area under the green bar.



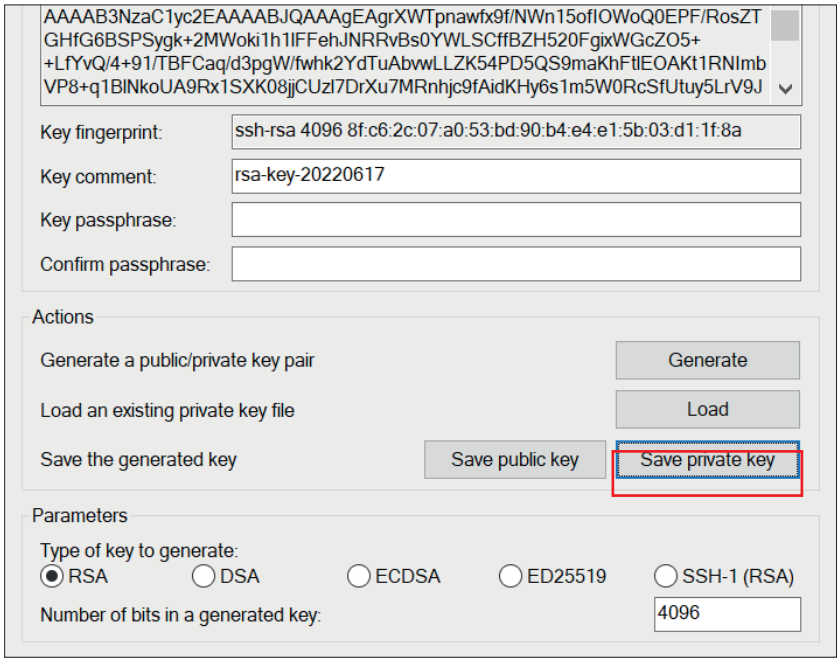
As soon as key generation is complete, the screen appears with the keys. Select *Save public key*.



Select *Save private key*.

Please note: the private key must be saved on your IT system, protected from unauthorized access and must NEVER be disclosed.

To protect the private key from unauthorized use, we recommend generating it with a passphrase. However, it should be noted that this can make it more difficult to automate registration, depending on the software used.



4.2 Creating an SSH key pair with OpenSSH

OpenSSH is a software package available on all Unix platforms. Further information can be found at http://www.openssh.com.

The SSH key pair can be generated with the following instruction:

```
ssh-keygen -b 4096 -t rsa -f /tmp/demo_key -C
"Commentary for Demo Key"
```

An example of the private key:

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

An example of the public key (this is automatically generated with the suffix .pub):

```
# cat /tmp/demo_key.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABA < --- SNIP --- > 6mEO5Gh28Vw== Comment for
Demo Key
```

4.3 Sending the public key to PostFinance

A copy of the public key must be sent to PostFinance by e-mail.

Service	E-mail address
Payment transactions	tscorp@postfinance.ch
Reconciliation file / RAF	aqs@postfinance.ch
Other	mftpf@postfinance.ch

So that PostFinance can verify the key they receive with the sender, the contact person must send the key (or the contact must be in the e-mail exchange). After receiving the public key, a PostFinance employee contacts the designated contact person to match the last characters of the public key hash value generated with SHA256. This ensures that no manipulation by a third party has taken place.

As soon as we have installed the key, we report completion to you. You can then test the connection.

Treat your private key like you treat your personal credit card! Protect it from unauthorized access.

4.4 Testing the connection

To test the connection, please select the desired host name for production or test environment (see section 3.2 *Host Name, Port and IP Addresses*).

The username and details of directory names and file names are communicated when the service is ordered.

4.4.1 Testing the connection with Telnet

The connection to MFTPF can be tested with Telnet:

```
# Telnet mftp1.postfinance.ch 8022
Trying mftp1.postfinance.ch...
Connected to mftp1.postfinance.ch.
Escape character is ,^]'.
SSH-2.0-SFTP Server
```

Note: Two IP addresses are used. Both IP addresses can be determined with several DNS resolution lookup requests (nslookup mftp1.postfinance.ch / nslookup mftt1.postfinance.ch). These IP addresses may be used only for configuring firewall rules. The DNS name must be used to make the connections.

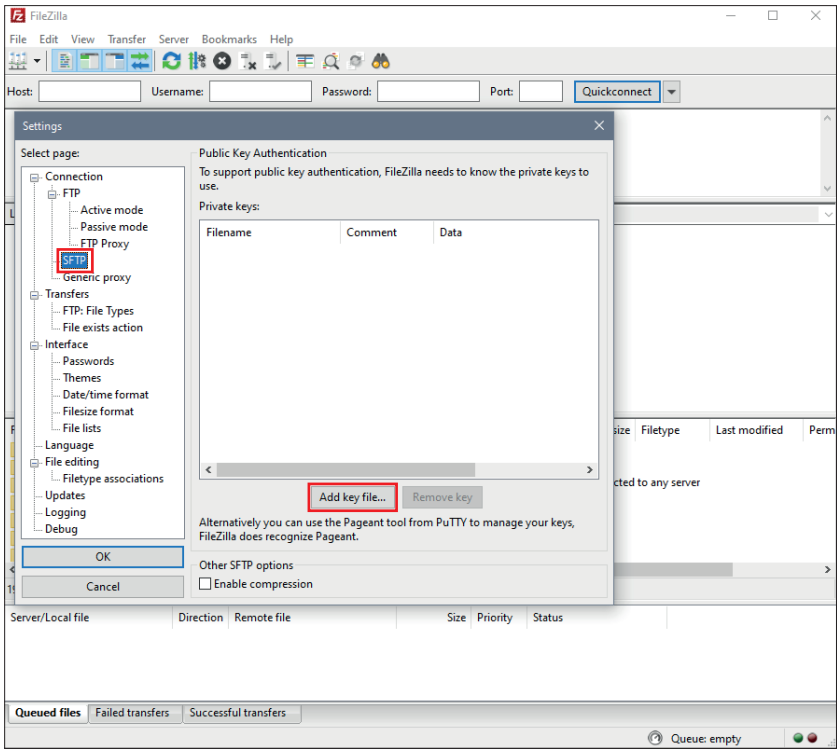
4.5 Configuring FileZilla

4.5.1 Key importing with FileZilla

The key for the import can be created with PuTTY or OpenSSH.

Start FileZilla.
Edit and then choose *settings*.
Select page: *SFTP*
Select *Add Key*.

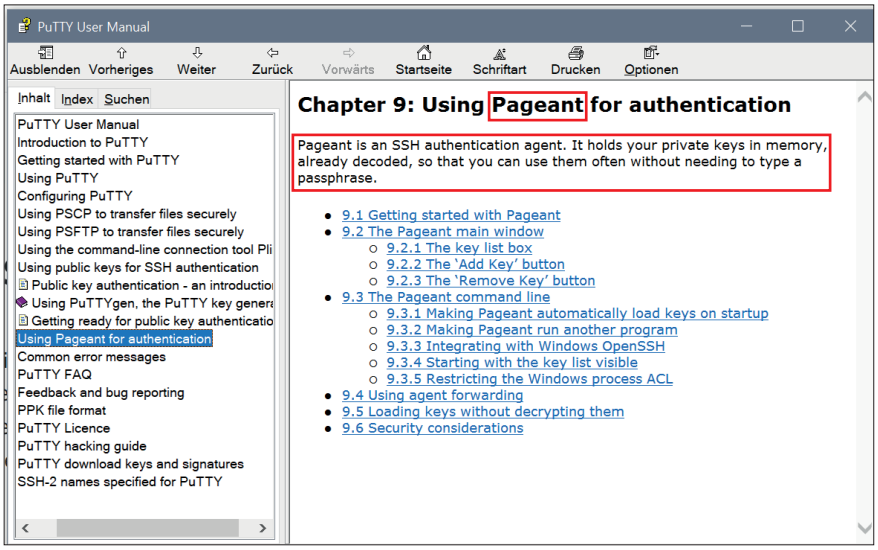
Add the previously generated private key.



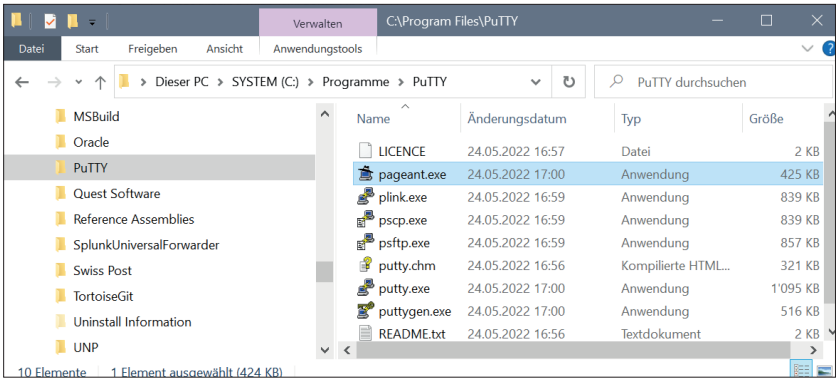
4.5.2 Automated importing with PuTTYs Pageant

Please note: To use PuTTYs Pageant, the key must be generated using PuTTY.

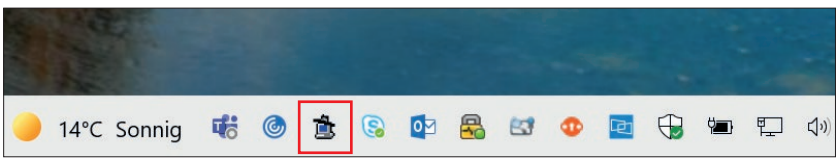
The *Pageant* (PuTTY Authentication Agent) is an SSH agent that can pass on SSH authentication. Pageant can load keys and provide them to local programs on request. The interface is open so that other programs can connect to this service from Pageant.



Start Pageant.exe.

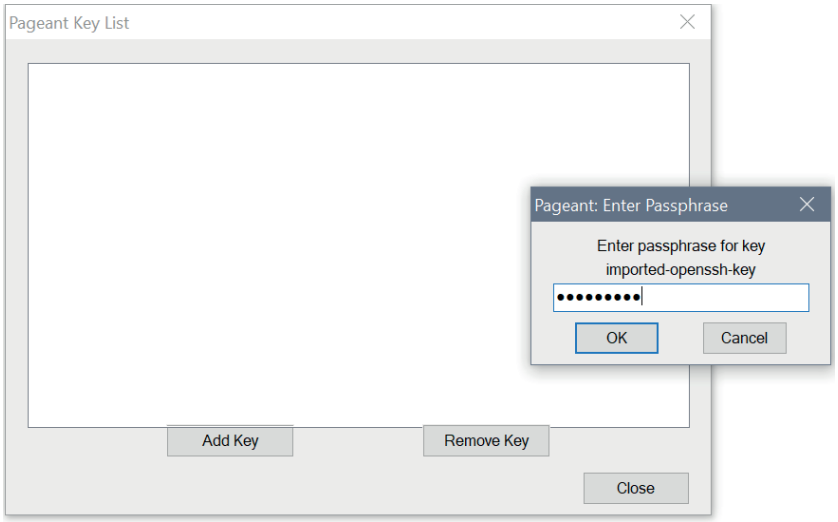


Pageant is located in the system tray in the bottom right in the quick launch bar and displays all sessions saved in Pageant.



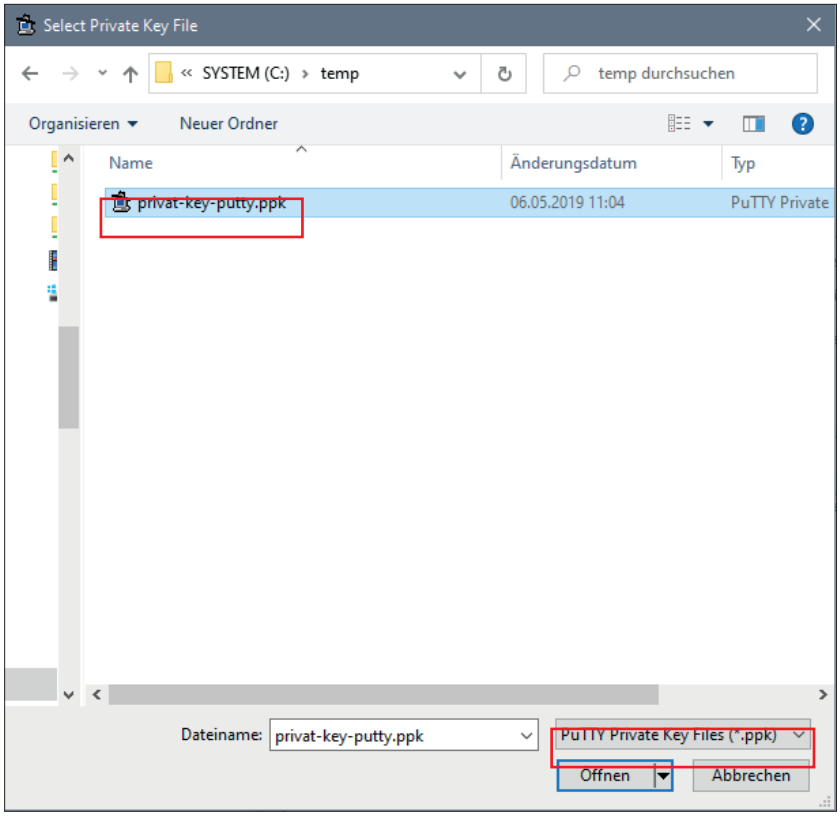
Double click on the "Hat" icon.

Use *Add Key* to open the window for selecting the private key.

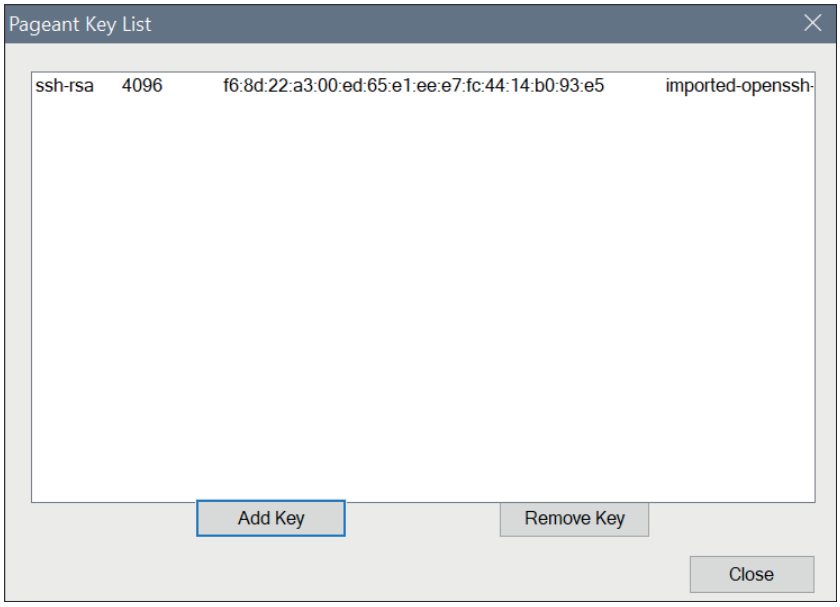


Select the private key and use *Open* to confirm.

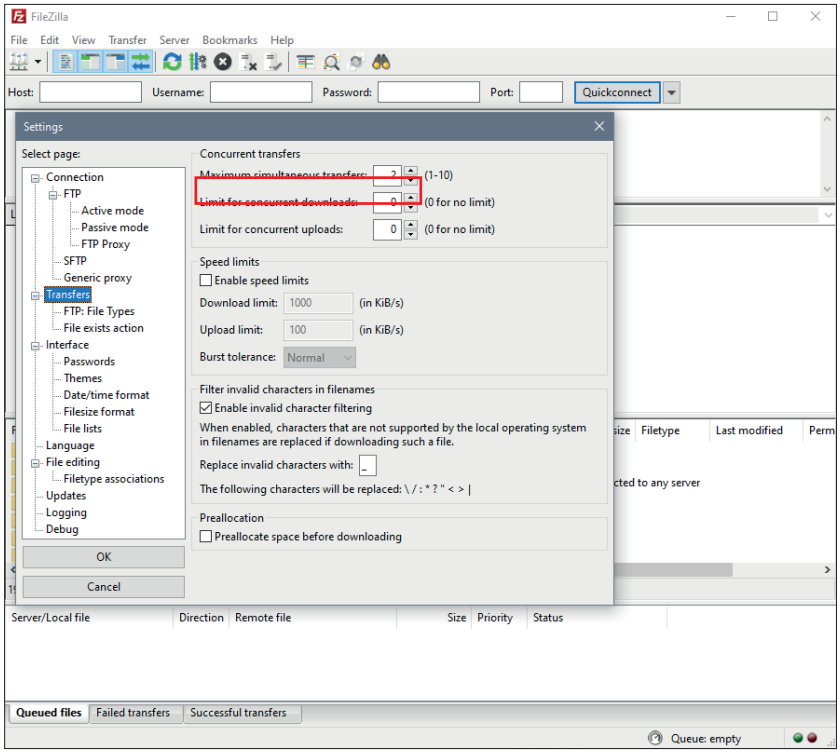
Please note: Only keys that have been generated using PuTTY can be applied.



The correctly imported key should look like the example alongside.



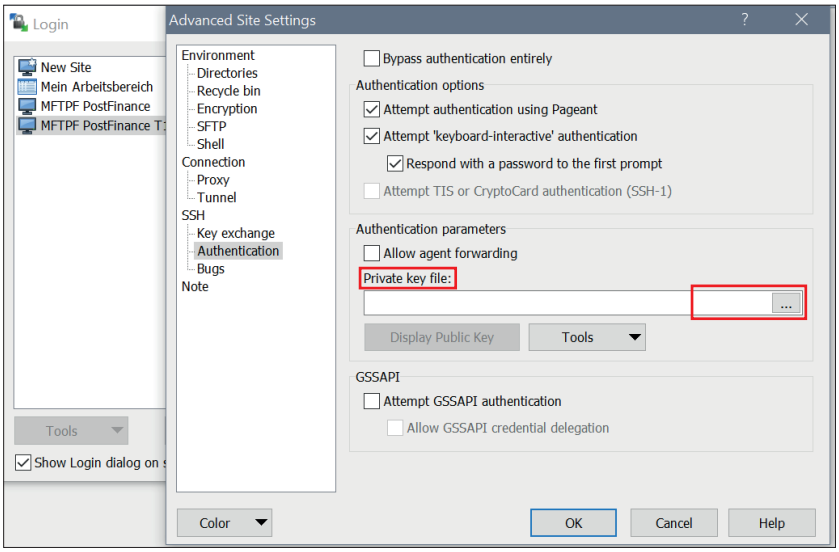
Note:
So as not to be locked out, we recommend setting the maximum number of simultaneous transfers to *three*.



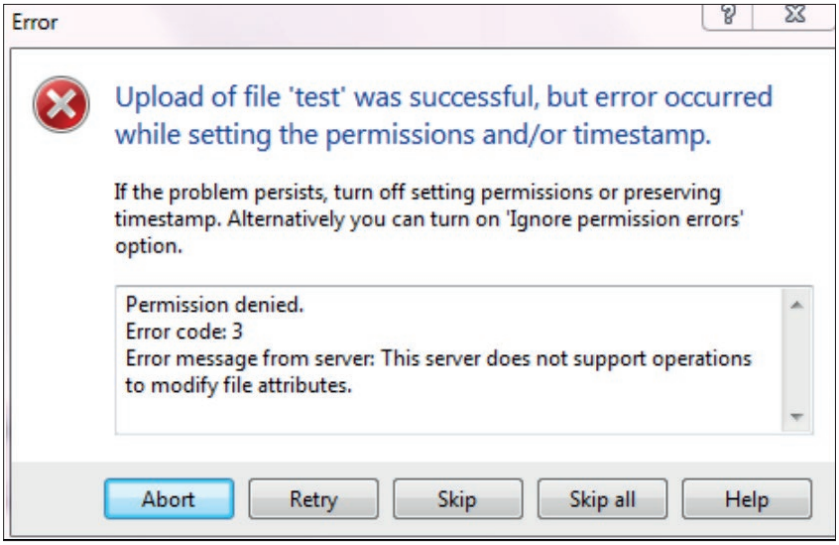
4.6 Configuring WinSCP

4.6.1 Key importing with WinSCP

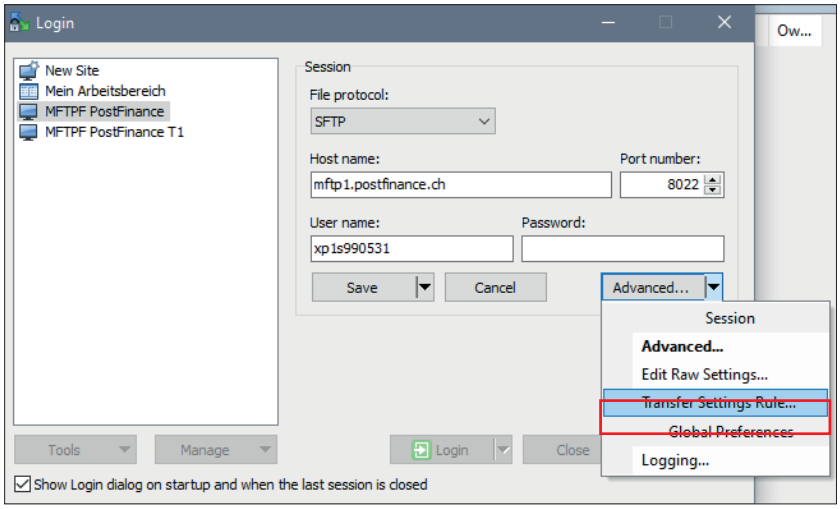
Start WinSCP.
Extended
Authentication
Click on *Private key file* […] and select the private key.



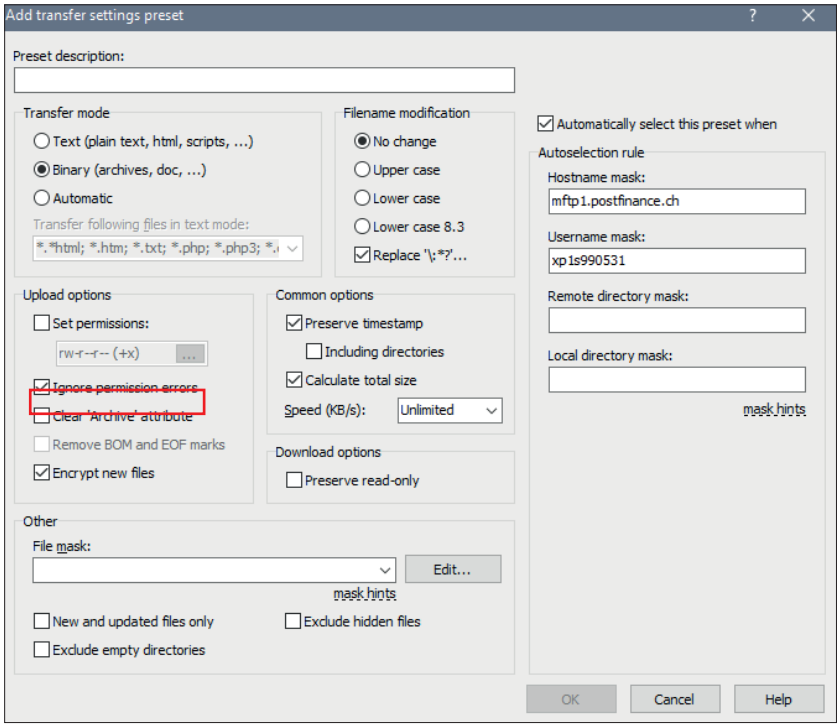
Problems with access after uploading as seen on the screen opposite can be rectified by adjusting the settings.



Go to
Advanced
Transfer Settings Rule
And select the required settings.



Activate
Ignore permission errors.



5. Information on using MFTPF

This brief information describes data exchange and the functions of MFTPF and presents generally valid rules and specifications for transferring files using the MFTPF servers.

5.1 Framework conditions/Restrictions

a) MFTPF is not an archiving system. Files for collection that the customer has not yet deleted are automatically removed from the server after nine days.
b) A large number of files must be transferred using a correspondingly large number of file transfers (put/get) for each SFTP login session. For example, with 1,200 files, 10 connections/logins each for 120 file transfers. If the number of logins during a given time unit is too great, the PostFinance's intrusion prevention system will automatically block the offending source IP address for 15 minutes.
c) MFTPF does not acknowledge the sender of a file transfer, i.e. MFTPF does not send a receipt notification on delivery of the files. Creating and sending receipts (e.g. pain.002 messages are provided for delivered pain.001 messages) is the task of the receiver system and is not guaranteed by MFTPF.
d) During file transfer, no transfer sequence is guaranteed during forwarding. Files of different sizes can overtake one another on a data transfer running in parallel. The receiver system in the end-to-end relationship is responsible for recreating the correct sequence of transferred files.
e) The forwarding and distribution of files is event-driven. It is not possible to control the timing.

Restrictions on data submission (Client → MFTPF server)
– For an upload function (put) for a file transfer client in an MFTPF directory, the files are processed in the operations on the MFTPF server directly after completion of the file transfers. However, the files entered in the Upload mailboxes remain visible to customers for 2 minutes (Use *dir* and *ls* to display the files). Deleting or renaming a sent file is ineffective; this file is forwarded to the recipient with the original file name.
– MFTPF ensures that only completely transferred files continue to be processed. If the connection is lost, the incomplete file is discarded.
– A change to file attributes after file transfer is not possible in MFTPF.