Handbuch
Managed File Transfer PostFinance (MFTPF)

PostFinance

499.81 de (pf.ch/dok.pf) 08.2022

Kundenbetreuung

Business Operations Support
Telefon +41 848 386 757
(im Inland max. CHF 0.08/Min.)
E-Mail tscorp@postfinance.ch

Technischer Support MFTPF
Telefon +41 (0)58 338 43 16
E-Mail mftpf@postfinance.ch

Impressum
PostFinance AG
3030 Bern

Version
August 2022

Inhaltsverzeichnis

1. Allgemeine Informationen

1.1 Zielgruppe des Kanals Managed File Transfer PostFinance (MFTPF)

Die PostFinance AG bietet ihren Kundinnen und Kunden für die Übermittlung und Abholung von Daten unterschiedliche Kanäle an. Der Managed File Transfer PostFinance (MFTPF) ist ein Kanal für den sicheren und automatisierten Datentransfer zwischen den Kunden und PostFinance zur effizienten Abwicklung des Zahlungsverkehrs sowie zum generellen Austausch von Daten. Die Dienstleistung richtet sich an Geschäftskunden, die regelmässig Daten (Zahlungsverkehrsdaten, Reconciliation Files / RAF, Software usw.) über einen sicheren Kanal mit PostFinance austauschen.

1.2 Gebrauch des Handbuchs

Dieses Handbuch beschreibt, wie Dateien mit dem MFTPF-Server der PostFinance AG ausgetauscht werden. Es richtet sich an die IT-Verantwortlichen, die den Verbindungsaufbau zwischen dem Kunden- und dem MFTPF-Server bei PostFinance etablieren.
Im ersten Teil des Handbuchs wird die Funktionalität des MFTPF-Servers beschrieben. Im zweiten Teil finden Sie die benötigten Konfigurationsparameter sowie eine Beschreibung, wie Sie die gängigsten SFTP Clients einrichten und das SSH-Key-Paar generieren.

1.3 Anwendbare Bestimmungen und Handbücher

Soweit das Handbuch Managed File Transfer PostFinance (MFTPF) keine besonderen Bestimmungen enthält, gelten die Allgemeinen Geschäftsbedingungen der PostFinance AG und die Teilnahmebedingungen digitales Leistungsangebot. Das vorliegende Handbuch sowie die Allgemeinen Geschäfts- und Teilnahmebedingungen von PostFinance können unter www.postfinance.ch/handbuecher heruntergeladen werden.

1.4 Anmeldung

Die Anmeldung für die Nutzung des MFTPF-Kanals erfolgt über Ihre Kundenberaterin bzw. Ihren Kundenberater oder über den Business Operations Support.

1.5 Vorgehen für die Nutzung des MFTPF-Kanals

Nach der Prüfung und Genehmigung Ihrer Anmeldung senden wir Ihnen Ihre MFTPF-User-ID.

Neben der MFTPF-User-ID benötigen Sie einen SFTP Client und ein SSH-Key-Paar, das Sie selbst erstellen können.
Bei der Wahl des Client sind Sie frei. Wir stellen Ihnen in diesem Handbuch zwei der gängigsten Clients (PuTTY und FileZilla) und deren Verbindungsmöglichkeiten vor.

1.6 Begriffe und Abkürzungen

Abkürzung	Definition
DMZ	DMZ steht für demilitarisierte Zone. Eine DMZ befindet sich an einem separaten LAN-Anschluss einer Firewall zwischen einem internen Netzwerk und einem unsicheren Netz (z. B. dem Internet). In der DMZ werden häufig Server, die Dienste für Internetnutzende (z. B. www oder Mail) zur Verfügung stellen, eingerichtet. Im Idealfall liegt eine DMZ zwischen zwei physikalisch getrennten Firewalls. Die äussere Firewall schützt vor Angriffen von aussen und kontrolliert jeglichen Internet-zugriff auf die DMZ. Die innere Firewall kontrolliert den Zugriff aus der DMZ in das interne Netzwerk und umgekehrt. Sie stellt somit eine zweite Verteidigungslinie dar, falls die äussere Firewall durchbrochen werden sollte. Dies hat den Vorteil, dass das interne Netz auch dann noch geschützt ist, wenn ein Angreifer bis zum Webserver gelangt.
DNS	Das Domain Name System (DNS) ist einer der wichtigsten Dienste im Internet. Seine Hauptaufgabe ist die Umsetzung von «Internetadressen» in die zugehörige IP-Adresse.
End-to-End	Bei End-to-End handelt es sich um die Beziehung zwischen einer Applikation der PostFinance AG und der Applikation des externen Kunden.
FileZilla	FileZilla ist ein FTP Client. Mit ihm lassen sich Daten über FTP-Server übertragen – einfach über FTP oder verschlüsselt über FTPS oder SFTP und per SSL oder SSH.
FTP	Das File Transfer Protocol (FTP) ist ein im RFC 959 von 1985 spezifiziertes Netzwerkprotokoll zur Dateiübertragung über TCP/IP-Netzwerke. Es ist ein Protokoll, das es erlaubt, Dateien zwischen verschiedenen Rechnern – unabhängig von ihrem Betriebssystem und Standort – auszutauschen.
GSLB	Der Global Server Load Balancing (GSLB) dient überwiegend der Verteilung der Zugriffe über eine zentrale Zugangsadresse auf geografisch entfernte Rechenzentren. Die GSLB-Technologie arbeitet nach den gleichen allgemeinen Grundsätzen wie der DNS-Lastausgleich.
IPSS	LAN Interconnect over IPSS ist eine Dienstleistung der Swisscom. Die Swisscom kann lokale Netzwerke zu einer einzigen unternehmensweiten Kommunikationsinfrastruktur vernetzen. IPSS ist eine Swisscom-eigene Lösung mit modernster Technologie. Die dabei verwendete MPLS-Technologie (Multi Protocol Label Switching) ermöglicht eine grosse Flexibilität hinsichtlich der Bandbreite. Der Dienst wird vollständig durch die Swisscom Enterprise Solution erbracht. Mehr Informationen unter: http://www.swisscom.com/es/
MAC	MAC (Message Authentification Code) ist ein auf symmetrischen Schlüsseln basierendes Kryptosystem mit dem Ziel, die Integrität von Meldungen zu garantieren.
MFTPF	Managed File Transfer PostFinance (MFTPF) ist ein Service, der den Empfang und den Versand von Dateien von und zu PostFinance beinhaltet.
MPLS	Beim Multi Protocol Label Switching (MPLS) handelt es sich um eine Implementation des Label Switching. Bei solchen Verfahren werden die am Transport eines Datenpakets beteiligten Router stark entlastet, da sich das Komplexitätsniveau auf das eines Switch reduziert. Dies wird erzielt, indem zu Beginn der Datenübertragung ein fester Verbindungsweg eingerichtet wird. Router auf diesem Weg müssen weiterzuleitende Datenpakete nicht mehr auf ihren Empfänger untersuchen, sondern geben diese ohne weitere Bearbeitung entsprechend des zuvor geschalteten Wegs weiter.
Public-Key-Verfahren	Das Public-Key-Verfahren ist ein asymmetrisches Kryptoverfahren, das aus einem öffentlichen (Public) und einem privaten (Private) Schlüssel besteht. Alle Benutzerinnen und Benutzer erzeugen ihr eigenes Schlüsselpaar, das aus einem geheimen Teil (privater Schlüssel) und einem nicht geheimen Teil (öffentlicher Schlüssel) besteht.
PuTTY	PuTTY ist ein freier SSH Client für Microsoft Windows.
SCP	SCP ist ein Protokoll zur verschlüsselten Übertragung von Daten zwischen zwei Computern über ein Rechnernetz.
SFTP	Secure File Transfer Protocol (SFTP), auch SSH File Transfer Protocol genannt, ist eine Weiterentwicklung von SCP und erlaubt eine sichere Datenübertragung und Dateizugriffe von einem Client auf entfernte Systeme. Das Protokoll beinhaltet weder die Authentifizierung noch die Verschlüsselung. Diese Funktionen müssen vom darunterliegenden SSH-Protokoll übernommen werden. SFTP ist nicht zu verwechseln mit Secure FTP oder mit FTP über SSL.
SSH	Secure Shell (SSH) bezeichnet sowohl ein Netzwerkprotokoll als auch die entsprechenden Programme, mit denen man auf eine sichere Art und Weise eine verschlüsselte Netzwerkverbindung mit einem entfernten Computer herstellen kann.
SSH-Key-Paar	Ein Schlüsselpaar, das aus einem geheimen Teil (privater Schlüssel) und einem nicht geheimen Teil (öffentlicher Schlüssel) besteht.
TTL	Die Time to Live (TTL, deutsch Lebenszeit) ist die Gültigkeitsdauer, die Daten in Rechnernetzen mitgegeben wird.
WinSCP	WinSCP ist eine freie SFTP- und FTP-Client-Software für Windows. WinSCP kopiert Dateien zwischen lokalen und entfernten Computern mit diversen Protokollen: FTP, FTPS, SCP, SFTP und WebDAV.

2. Der Managed File Transfer PostFinance (MFTPF)

2.1 Überblick

Der Managed File Transfer PostFinance (MFTPF) ist der Kanal für den Filetransfer zwischen PostFinance und ihren Kundinnen und Kunden und Partnern. Der MFTPF ersetzt ab sofort das Produkt FDS bei PostFinance.

2.2 Aufbau

MFTPF setzt sich aus mehreren Applikations-, Datenbank- und Perimeterservern zusammen. Alle Komponenten stehen in verschiedenen Zonen. Die Filetransfer- und Datenbankserver stehen in einer hochgeschützten Zone, auf die der Zugriff nur sehr beschränkt möglich ist. Die von extern zugänglichen File-Server, bei uns Secure-Transport-Edge-Server genannt, stehen in weniger hochgeschützten Zonen, auf die der Zugriff mit Clients erlaubt ist (DMZ). Die Client-/Server-Verbindungen aus den externen Netzwerken laufen immer über die Secure-Transport-Edge-Server.

MFTPF ist georedundant ausgelegt. Bei einem allfälligen Ausfall eines Rechenzentrums steht er trotzdem weiter zur Verfügung.

2.3 Anschluss

2.3.1 Secure File Transfer Protocol (SFTP)

Für den Filetransfer zwischen PostFinance und den Kundinnen und Kunden / Partnern wird ausschliesslich SFTP benutzt. SFTP (Secure File Transfer Protocol) ist ein sicheres Filetransfer-Protokoll. Zwischen Client und Server wird eine ununterbrochene, verschlüsselte Verbindung hergestellt, die die Benutzernamen und Daten für Angreifer unlesbar macht. Für die Authentifizierung wird das Public-Key-Verfahren angewendet. Somit kann sich der Client ohne Benutzerinteraktion auf dem Server einloggen.
SSH garantiert das vollständige und unveränderte Übertragen der Daten vom Absender zum Empfänger.

MFTPF unterstützt die SSH-2 (Version 2).

Achtung: SFTP ist nicht mit FTPS (FTP über SSL) oder mit FTP über SSH zu verwechseln!

2.3.2 Empfohlene Clients

PostFinance empfiehlt die gängigsten Clients WinSCP und FileZilla. Die Konfiguration wird im Kapitel 4 aufgezeigt.

2.3.3 Anschlussarten

Der Filetransfer erfolgt in der Regel über das Internet.

Für andere Anschlussarten wie Mietleitungen (MPLS/IPSS) wenden Sie sich bitte an das Team Technischer Support MFTPF. Die Kontaktangaben finden Sie unter «Kundenbetreuung» am Anfang des Handbuchs.

2.4 Ein- und Auslieferung

Den Kundinnen und Kunden stehen auf dem MFTPF-Server verschiedene Verzeichnisse für die Ein- und Auslieferung zur Verfügung.
Die Auslieferung und Verteilung einer Datei erfolgt ereignisorientiert. Nach dem Eingang einer Datei wird diese vom MFTPF-Server an die vorbestimmten Destinationen weitergeleitet. Das Festlegen eines bestimmten Zeitpunkts für die Ausführung einer Aktion ist nicht möglich.

Ein- und Auslieferungen von Dateien an ein externes Zielsystem (Kundenserver) durch PostFinance sind möglich. Um einen reibungslosen Betrieb sicherstellen zu können, sind folgende kundenseitige Voraussetzungen zu erfüllen:
- Infrastruktur und Rechenzentrum-Betrieb sind 24/7 verfügbar
- Ansprechstellen für den Support (Telefonnummern, E-Mail) sind 24/7 erreichbar

3. Konfigurationsparameter

Das nachfolgende Kapitel gibt eine Übersicht über die Konfigurations-parameter.

3.1 SFTP-Voraussetzungen

Der MFTPF-Server unterstützt:
- Version 2: SSH Protocol
- Version 3: SFTP Protocol
- Eingehende SCP-Befehle mit SSH/SCP-Protokoll (Achtung: SCP unterstützt die Befehle *list, rename* und *delete* nicht.)
- Verschlüsselungs-Algorithmen: AES mit Schlüssellänge mind. 128 Bits
- Message Authentication Codes (MAC): hmac-sha2-256
- Übertragungen von Dateien mit einer Grösse von bis zu 50 Gigabytes
- 50 gleichzeitige Verbindungen vom gleichen Account
- Sperrung des Accounts nach 5 fehlerhaften Loginversuchen (Bitte melden Sie sich beim Team Technischer Support MFTPF, um den Account wieder freizuschalten.)
- Unterstützt werden Keys in den Formaten OpenSSH, ssh.com und PuTTY
- Pro Account können ein oder mehrere Keys konfiguriert werden

3.2 Host-Name, Port und IP-Adressen

Umgebung	Host-Name	Port
Produktion	mftp1.postfinance.ch	8022
Test 1	mftt1.postfinance.ch	8022
Test 2	mftt2.postfinance.ch	8022

Die Verteilung der Kommunikation über zwei Standorte wird mit DNS Loadbalancing (Round-Robin) erreicht. Dies bedeutet, dass abwechselnd die IP-Adressen der beiden Standorte zurückgegeben werden.

Es muss sichergestellt werden, dass die Kommunikation zu oder ab MFTPF in Ihrem Netzwerk erlaubt ist. In vielen Fällen muss das Netzwerk-Team die Verbindungen mit entsprechenden Firewall-Regeln erlauben. Es werden zwei IP-Adressen verwendet. Die IP-Adressen dürfen nur für die Konfiguration von Firewall-Regeln gebraucht werden. Für den Verbindungsaufbau ist zwingend der DNS-Name zu benutzen.

Die beiden IP-Adressen können mit DNS-Auflösung (nslookup mftp1.postfinance.ch) durch mehrere Versuche ermittelt werden. MFTPF unterstützt IPv4 und IPv6. Die Verwendung von IPv6 erfordert eine durchgehende IPv6-Unterstützung in Ihrer Infrastruktur.

3.3 DNS Caching

Die Plattform wird mit einer Active / Active Konfiguration über zwei Standorte betrieben. Der Failover-Mechanismus wird mit einer *Global Server Load Balancing (GSLB)*-Infrastruktur sichergestellt. Damit Sie von einem raschen Failover der Verbindung zu MFTPF profitieren können, müssen Sie in Ihrer Umgebung sicherstellen, dass kein zusätzliches DNS Caching gemacht wird. Die Angabe zur Time to Live (TTL) vom PostFinance-DNS muss zwingend respektiert werden.

3.4 Autorisierung

Für die Verbindung auf dem MFTPF-Server wird der Benutzername (MFTPF-User-ID) und ein gültiges SSH-Key-Paar benötigt.

Benutzernamen (MFTPF-User-ID)
Der Benutzername wird im Rahmen der Bestellung des MFTPF-Kanals kommuniziert.

Public Key
Der SSH Key muss mindestens 4096 Bits lang sein. Das Kryptosystem ist RSA.

Falls erwünscht, besteht die Möglichkeit, mehrere Public Keys für den gleichen Benutzernamen zu konfigurieren. Ebenso können mehrere Benutzerinnen und Benutzer den gleichen Key verwenden.

Eine Kopie des Public Key muss PostFinance gemäss der Anmeldung gesendet werden.

3.5 Verzeichnisse

Die Verzeichnisse werden durch PostFinance erstellt. Die Benutzerinnen und Benutzer können die Verzeichnisse weder erstellen noch löschen.

Die Syntax der Verzeichnisse enthält folgende Zeichen:
– Zeichen: [a–z], [0–9], [. -] (Punkt, Bindestrich)
– Beginn: Das erste Zeichen muss [a–z], [0–9] sein

Die für Sie relevanten Verzeichnisse geben wir Ihnen mit der Anmeldung des Kanals bekannt.

3.6 Dateinamen

Für die Dateinamen dürfen folgende Zeichen verwendet werden:
– Zeichen: [A–Z], [a–z], [0–9], [. - _] (Punkt, Bindestrich, Unterstrich)

Die Dateinamen, die von PostFinance vergeben werden, unterscheiden sich je nach Dienstleistung, sie berücksichtigen aber die vorgängig beschriebene Syntax.
Bitte beachten Sie, dass Dateien, die Sie erstellen, diese Syntax zwingend einhalten müssen. Nur so können wir garantieren, dass die Dateien verarbeitet werden.

4. Erstellen der SSH Keys und Einrichten des Client

In diesem Kapitel wird aufgezeigt, wie die SSH Keys mit PuTTY und OpenSSH generiert und die gängigsten Clients FileZilla und WinSCP für den Filetransfer konfiguriert werden.

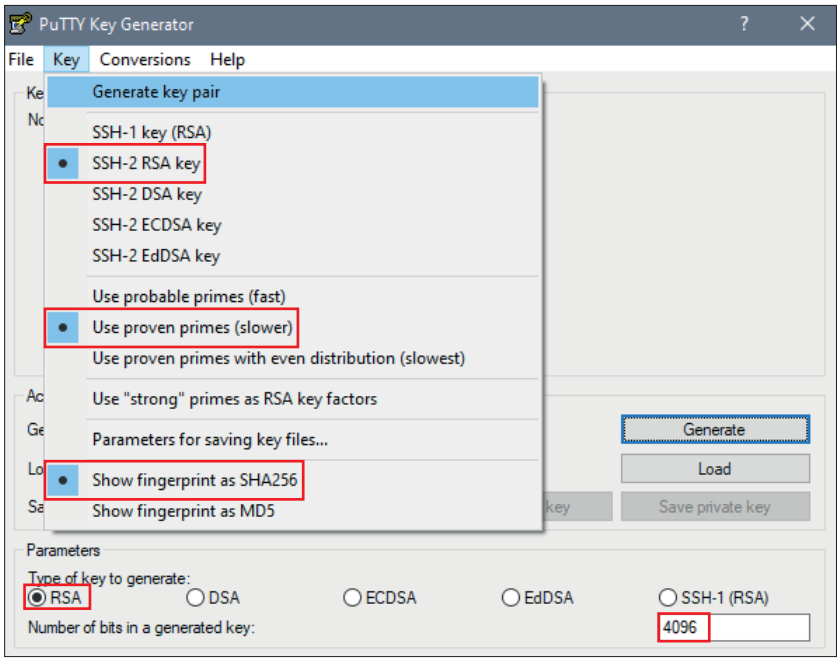
4.1 Erstellen eines SSH-Key-Paars mit PuTTY

PuTTY ist eine Open Source Software für Microsoft Windows. Sie kann unter http://www.putty.org heruntergeladen werden.
Mit dem SSH/SFTP Client (putty.exe) können der Private und der Public Key separat generiert werden. Mit PuTTYgen besteht die Möglichkeit, Key-Paare zu generieren.

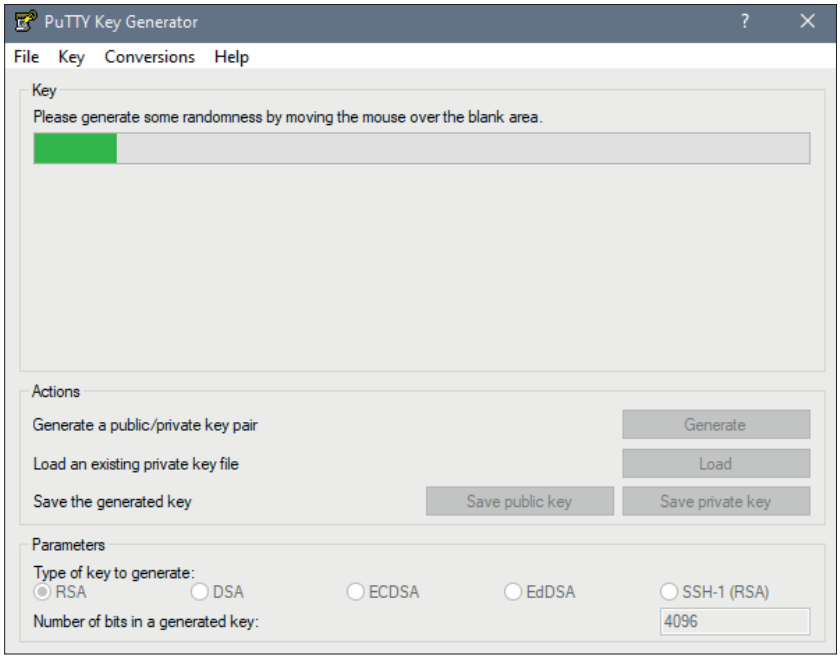
PuTTYgen starten.

SSH-2 RSA als Schlüssel-Typ wählen.
4096 Bits als Länge eingeben.

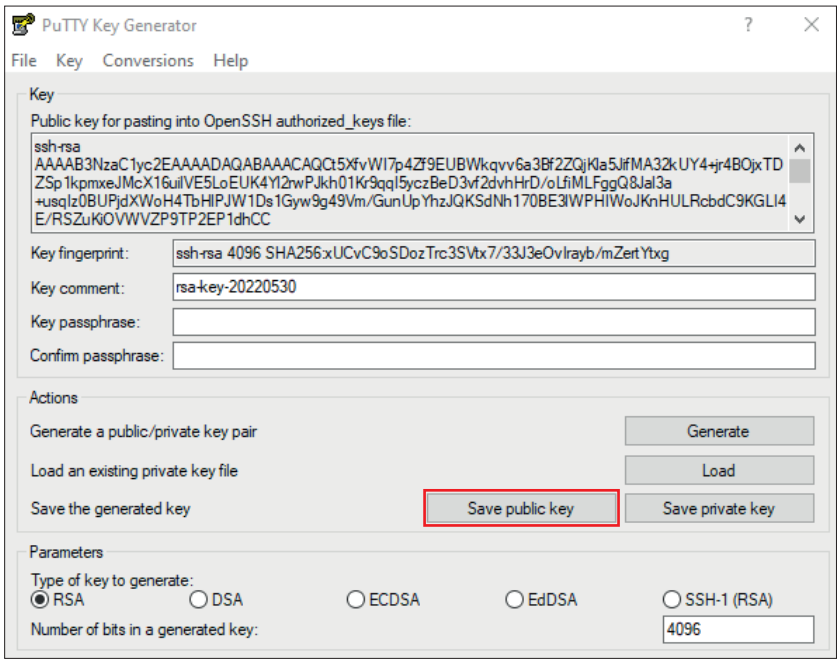
Generate anklicken.



Mit dem Cursor der Maus über die Fläche unter dem grünen Balken fahren.



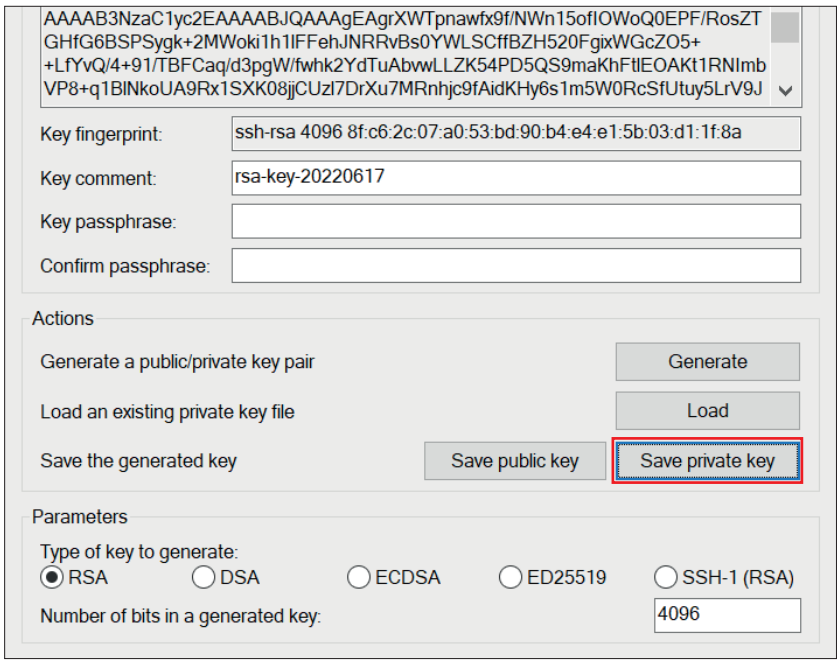
Sobald die Generierung des Key abgeschlossen ist, erscheint die Maske mit den Keys.
Save public key wählen.



Save private key wählen.

Achtung: Der Private Key muss auf Ihrem IT-System gespeichert, vor unberechtigtem Zugriff geschützt und darf NIE weitergegeben werden.

Damit der Private Key vor unberechtigtem Gebrauch geschützt ist, wird empfohlen, ihn mit einer Passphrase zu generieren. Es muss beachtet werden, dass – je nach eingesetzter Software – die Automatisierung der Anmeldung dadurch erschwert werden kann.



4.2 Erstellen eines SSH-Key-Paars mit OpenSSH

OpenSSH steht als Programmpaket auf allen Unix-Plattformen zur Verfügung. Weitere Informationen über OpenSSH sind unter http://www.openssh.com zu finden.

Das SSH-Key-Paar kann mit folgendem Befehl generiert werden:

```
ssh-keygen -b 4096 -t rsa -f /tmp/demo_key -C
„Kommentar fuer Demo Key“
```

Hier ein Beispiel des Private Key:

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

Hier ein Beispiel des Public Key (dieser wird automatisch mit dem Suffix .pub generiert):

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

4.3 Senden des Public Key an PostFinance

Eine Kopie des Public Key muss PostFinance per E-Mail zugestellt werden.

Dienstleistung	E-Mail-Adresse
Zahlungsverkehr	tscorp@postfinance.ch
Reconciliation Files / RAF	aqs@postfinance.ch
Andere	mftpf@postfinance.ch

Damit PostFinance den erhaltenen Key mit der Absenderin bzw. dem Absender verifizieren kann, muss die Kontaktperson den Key senden (oder der Kontakt muss im E-Mail-Austausch vorkommen). Nach Erhalt des Public Key kontaktiert ein bzw. eine Mitarbeitende/-r von PostFinance die angegebene Kontaktperson, um die letzten Stellen des mit SHA256 generierten Hash-Werts des Public Key abzugleichen. Somit kann sichergestellt werden, dass keine Manipulation durch eine Drittpartei stattgefunden hat.

Sobald wir den Key installiert haben, melden wir Ihnen den Abschluss. Sie können danach die Verbindung testen. Wenn Sie Unterstützung benötigen, können Sie sich beim Team Technischer Support MFTPF melden.

Behandeln Sie Ihren Private Key wie Ihre persönliche Kreditkarte! Schützen Sie ihn vor unberechtigten Zugriffen.

4.4 Testen der Verbindung

Für den Test der Verbindung wählen Sie bitte den gewünschten Host-Namen für Produktion oder Testumgebung aus (siehe Kapitel 3.2 *Host-Name, Port und IP-Adressen*).

Der Benutzername sowie Details zu Verzeichnisnamen und Dateinamen werden im Rahmen der Service-Bestellung kommuniziert.

4.4.1 Test der Verbindung mit Telnet

Die Verbindung zu MFTPF kann zum Beispiel mit Telnet überprüft werden:

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

Achtung: Es werden zwei IP-Adressen verwendet. Die beiden IP-Adressen können mit DNS-Auflösung (nslookup mftp1.postfinance.ch bzw. nslookup mftt1.postfinance.ch) durch mehrere Versuche ermittelt werden. Die IP-Adressen dürfen nur für die Konfiguration von Firewall-Regeln verwendet werden. Für den Verbindungsaufbau ist zwingend der DNS-Name zu benutzen.

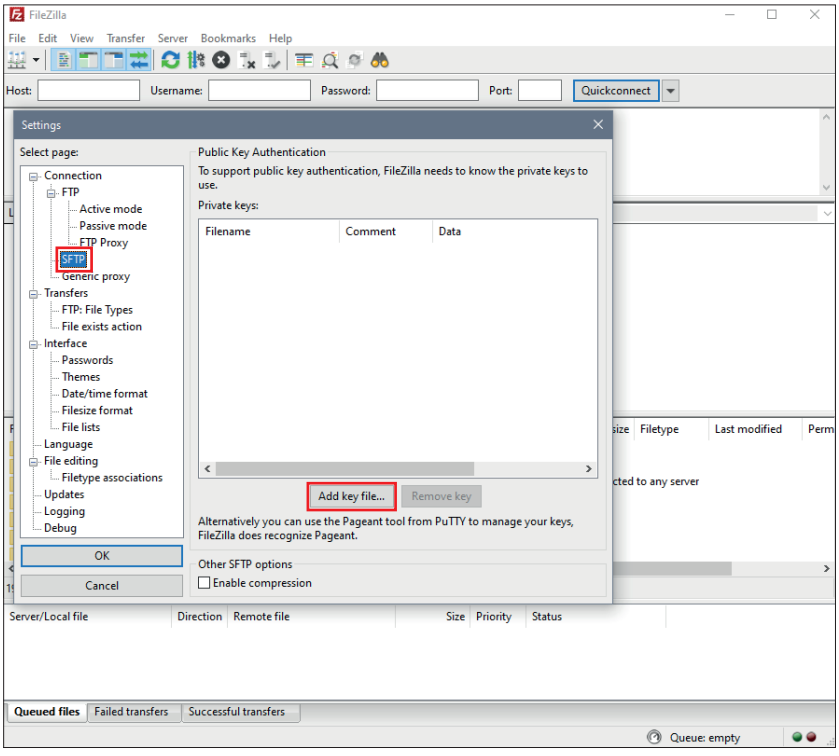
4.5 Konfiguration FileZilla

4.5.1 Key importieren mit FileZilla

Für den Import kann der Key mit PuTTY oder OpenSSH erstellt werden.

FileZilla starten.
Bearbeiten und dann *Einstellungen* wählen.
Seite auswählen: *SFTP*
Schlüssel hinzufügen wählen.

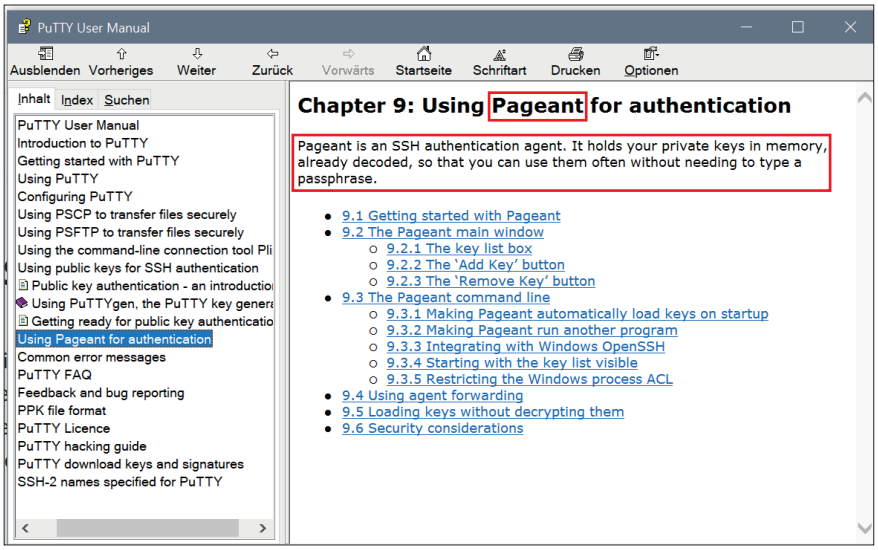
Den zuvor generierten Private Key hinzufügen.



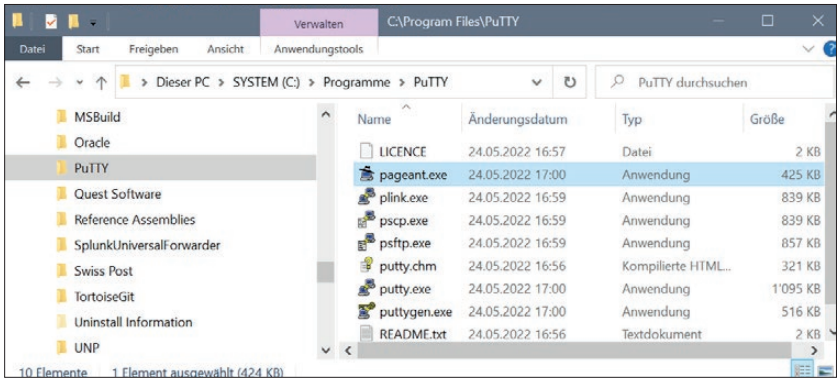
4.5.2 Automatisches Importieren mit PuTTYs Pageant

Achtung: Um PuTTYs Pageant zu verwenden, muss der Key mit PuTTY generiert werden.

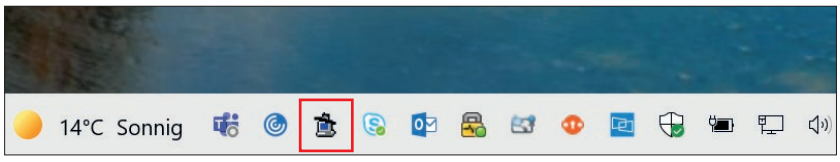
Der *Pageant* (PuTTY Authentication Agent) ist ein SSH-Agent, mit dem SSH-Authentifizierungen weitergereicht werden können. Pageant kann Schlüssel laden und diese lokalen Programmen auf Anfrage zur Verfügung stellen. Die Schnittstelle ist offen, sodass sich weitere Programme an diese Dienstleistung von Pageant anbinden können.



Pageant.exe starten.

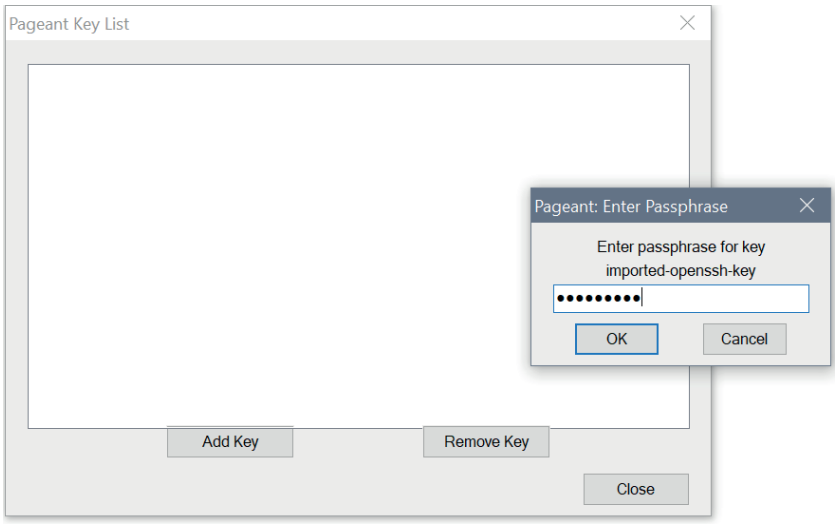


Pageant befindet sich im System-Tray rechts unten in der Schnellstart-Leiste und zeigt alle in Pageant gespeicherten Sessions an.



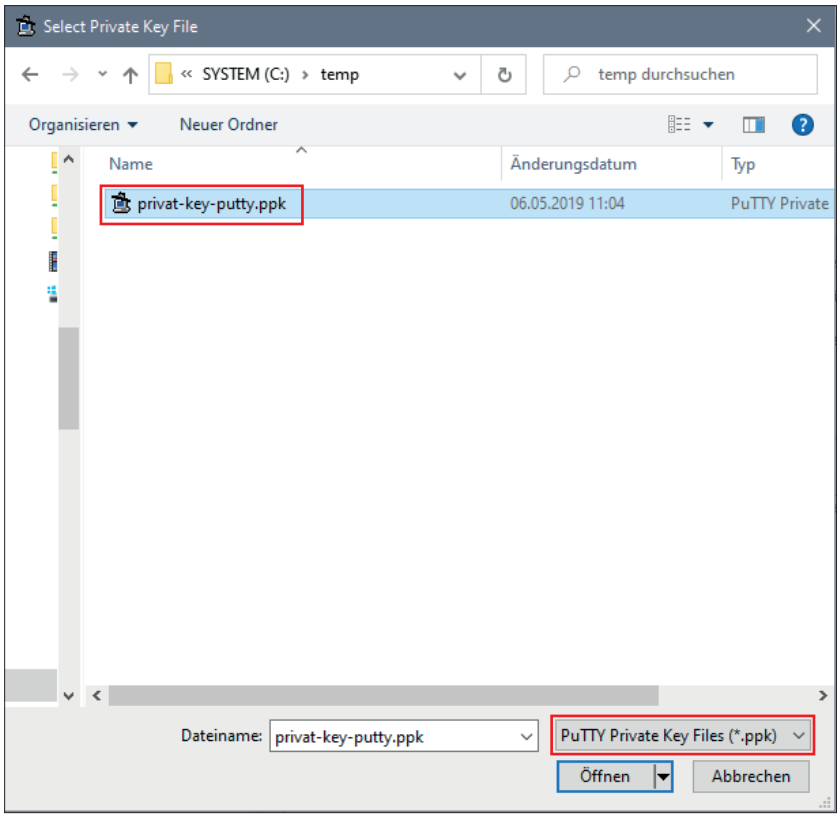
Doppelklick auf «Hut»-Icon.

Mit *Add Key* das Fenster zur Auswahl des Private Key öffnen.

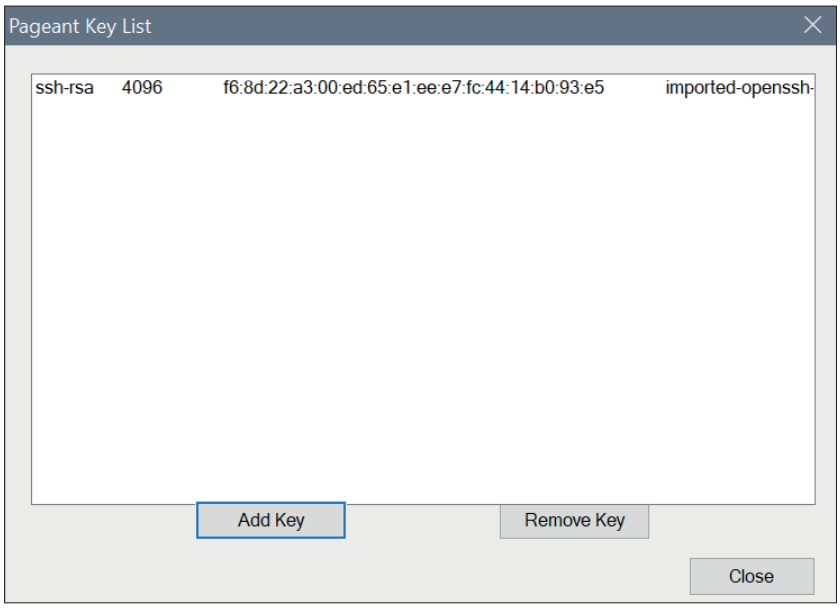


Den Private Key auswählen und mit *Öffnen* bestätigen.

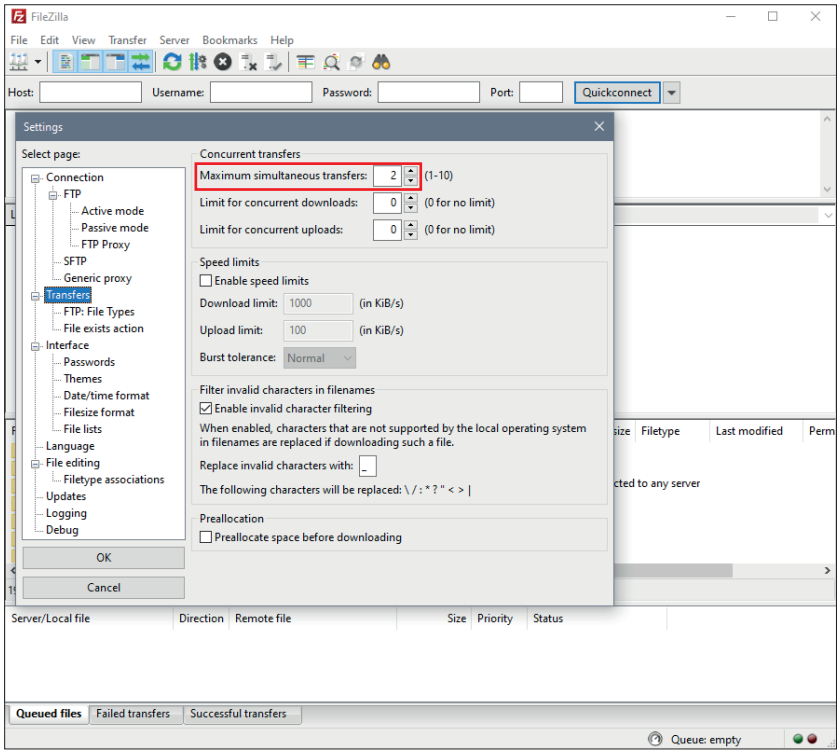
Achtung: Es können nur Keys, die mit PuTTY generiert wurden, übernommen werden.



Der korrekt importierte Key sollte wie im nebenstehenden Beispiel aussehen.



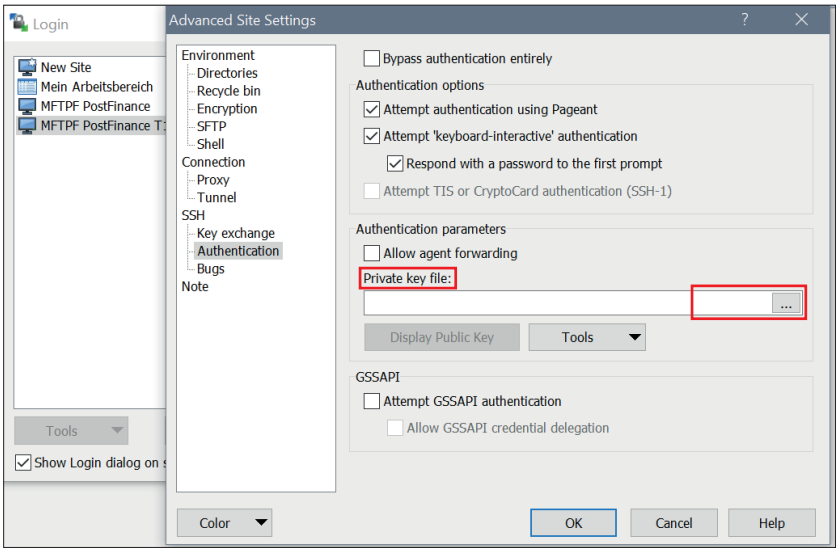
Hinweis:
Um nicht ausgesperrt zu werden, empfehlen wir, die maximale Anzahl gleichzeitiger Übertragungen auf *drei* zu setzen.



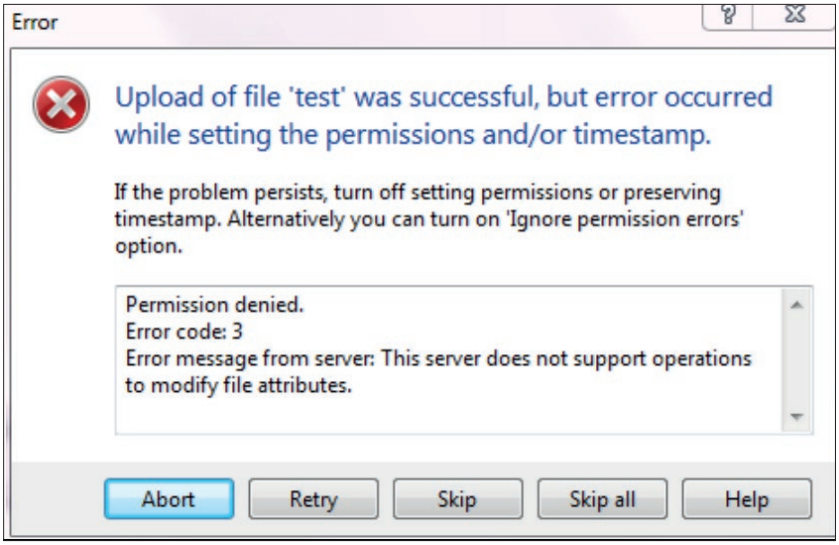
4.6 Konfiguration WinSCP

4.6.1 Key importieren mit WinSCP

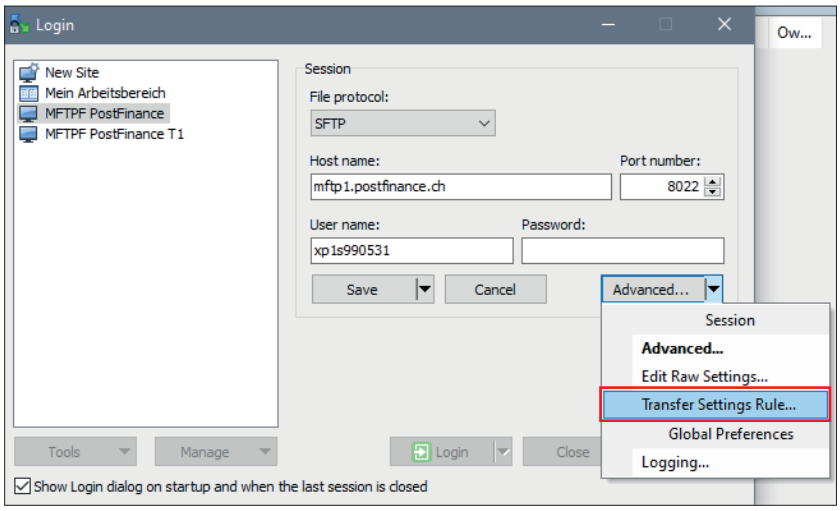
WinSCP starten.
Erweitert
Authentifizierung
Unter *Datei mit privatem Schlüssel* […] anklicken und den Private Key auswählen.



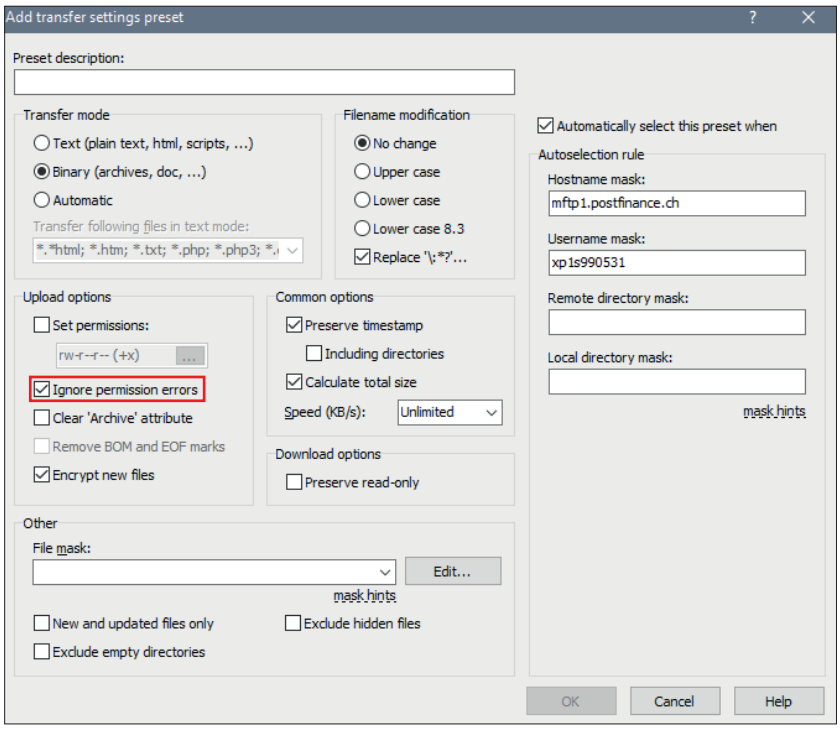
Probleme mit den Berechtigungen nach dem Hochladen gemäss dem nebenstehenden Screen können mit Anpassungen der Einstellungen behoben werden.



Gehen Sie zu
Erweitert
Regel für Übertragungseinstellungen
Und wählen Sie diese aus.



Aktivieren Sie
Berechtigungsfehler ignorieren.



5. Informationen zur Anwendung MFTPF

Die vorliegende Kurzinformation beschreibt den Datenaustausch und die Funktionen von MFTPF und stellt allgemeingültige Regeln und Vorgaben für die Übertragung von Dateien mit den MFTPF-Servern auf.

5.1 Rahmenbedingungen/Einschränkungen

a) MFTPF ist kein Archivierungssystem. Abzuholende Dateien, die die Kundin bzw. der Kunde noch nicht gelöscht hat, werden in jedem Fall nach neun Tagen vom Server automatisch entfernt.
b) Eine grosse Anzahl von Dateien muss mit einer entsprechend grossen Anzahl von Filetransfers (put/get) pro SFTP Login Session übertragen werden. Beispiel für 1200 Files: zehn Verbindungen/Logins mit je 120 Filetransfers. Wird die Anzahl der Logins während einer bestimmten Zeiteinheit zu gross, sperrt das Intrusion Prevention System von PostFinance die verursachende Source-IP-Adresse automatisch während 15 Minuten.
c) MFTPF quittiert den Absenderinnen und Absendern den Filetransfer nicht, d. h. MFTPF sendet ihnen keine Empfangsmeldung beim Einliefern von Dateien. Das Erstellen und Versenden von Quittungen (z. B. für eingelieferte pain.001-Meldungen werden pain.002-Meldungen bereitgestellt) ist Aufgabe der Empfangssysteme und wird nicht von MFTPF sichergestellt.
d) Beim Filetransfer ist bei Weiterleitungen keine Übertragungsreihenfolge garantiert. Dateien unterschiedlicher Grösse können sich bei einer parallel laufenden Datenübertragung überholen. Das Empfangssystem der End-to-End-Beziehung ist für die Wiederherstellung der richtigen Reihenfolge der übertragenen Dateien zuständig.
e) Die Weiterleitung und Verteilung von Dateien ist ereignisgesteuert. Eine zeitliche Steuerung ist nicht möglich.

Einschränkungen bei der Dateneinlieferung (Client → MFTPF-Server)
- Bei einer Upload-Funktion (put) eines Filetransfer-Client in ein MFTPF-Verzeichnis werden die Dateien von den Prozessen auf dem MFTPF-Server unmittelbar nach Abschluss des Filetransfers bearbeitet. Die Einträge der Dateien in den Upload-Mailboxen bleiben jedoch für die Kundinnen und Kunden während 2 Minuten ersichtlich (Anzeige der Dateien mit *dir* und *ls*). Die Löschung oder die Umbenennung einer gesendeten Datei ist wirkungslos: diese Datei wird mit dem ursprünglichen Dateinamen an die Empfängerin bzw. den Empfänger weitergeleitet.
- MFTPF stellt sicher, dass nur vollständig übermittelte Dateien weiterverarbeitet werden. Im Fall eines Verbindungsabbruchs wird die unvollständige Datei verworfen.
- Eine Änderung der Datei-Attribute nach dem Filetransfer ist auf MFTPF nicht möglich.