Manuel
Managed File Transfer PostFinance (MFTPF)

PostFinance

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

Service à la clientèle

En cas de questions sur les produits PostFinance et les canaux du trafic des paiements, votre conseillère ou votre conseiller à la clientèle se tient à votre disposition.

Vous pouvez également vous adresser à notre **conseil Clientèle commerciale:**
Conseil et vente
Téléphone +41 848 888 900
(max. CHF 0.08/min. en Suisse)

Impressum
PostFinance SA
3030 Berne

Version
Mai 2023

Sommaire

1.	**Informations générales**	**4**
1.1	Groupe cible du canal Managed File Transfer PostFinance (MFTPF)	4
1.2	Utilisation du manuel	4
1.3	Dispositions et manuels applicables	4
1.4	Adhésion	4
1.5	Procédure d'utilisation du canal MFTPF	4
1.6	Termes et abréviations	5
2.	**Le Managed File Transfer PostFinance (MFTPF)**	**6**
2.1	Vue d'ensemble	6
2.2	Mise en place	6
2.3	Branchement	6
2.3.1	Secure File Transfer Protocol (SFTP)	6
2.3.2	Clients recommandés	6
2.3.3	Types de raccordement	6
2.4	Réception et livraison des données	7
3.	**Paramètres de configuration**	**8**
3.1	Prérequis SFTP	8
3.2	Nom de l'hôte, port et adresses IP	8
3.3	Cache DNS	9
3.4	Autorisation	9
3.5	Répertoires	9
3.6	Noms de fichiers	9
4.	**Créer les clés SSH et générer le client**	**10**
4.1	Créer une paire de clés SSH avec PuTTY	10
4.2	Créer une paire de clés SSH avec OpenSSH	11
4.3	Envoyer la clé publique à PostFinance	12
4.4	Tester la connexion	13
4.4.1	Test de la connexion avec Telnet	13
4.5	Configuration FileZilla	13
4.5.1	Importer une clé avec FileZilla	13
4.5.2	Importation automatique avec PuTTY's Pageant	14
4.6	Configuration WinSCP	17
4.6.1	Importer une clé avec WinSCP	17
5.	**Informations sur l'utilisation MFTPF**	**19**
5.1	Conditions-cadres/Restrictions	19

1. Informations générales

1.1 Groupe cible du canal Managed File Transfer PostFinance (MFTPF)

PostFinance SA offre à ses clientes et ses clients différents canaux pour la transmission et le retrait de données. Le Managed File Transfer PostFinance (MFTPF) est un canal de transfert de données sécurisé et automatisé entre la clientèle et PostFinance qui traite de manière efficace le trafic de paiements et l'échange général de données. Cette prestation s'adresse aux clients commerciaux qui échangent régulièrement des données (données du trafic des paiements, Reconciliation Files/RAF, logiciels, etc.) par le biais d'un canal sécurisé de PostFinance.

1.2 Utilisation du manuel

Ce manuel décrit la manière dont les fichiers peuvent être échangés avec le serveur MFTPF de la PostFinance SA. Il s'adresse aux responsables IT qui établissent la liaison entre le client et le serveur MFTPF de PostFinance. La première partie du manuel décrit la fonctionnalité du serveur MFTPF. Dans la deuxième partie, vous trouverez les paramètres de configuration nécessaires ainsi qu'une description pour générer les clients SFTP les plus courants et la paire de clés SSH.

1.3 Dispositions et manuels applicables

Sauf dispositions contraires dans le manuel Managed File Transfer PostFinance (MFTPF), les conditions générales de PostFinance SA et les Conditions de participation Offre de prestations numériques s'appliquent. Le présent manuel ainsi que les conditions générales et conditions de participation de PostFinance peuvent être téléchargés sous www.postfinance.ch/manuels.

1.4 Adhésion

L'adhésion au canal MFTPF peut se faire auprès de votre conseillère ou votre conseiller à la clientèle ou auprès du Customer Center.

1.5 Procédure d'utilisation du canal MFTPF

Après contrôle et approbation de votre demande d'adhésion, nous vous envoyons votre User ID MFTPF.

En plus du User ID MFTPF, vous avez besoin d'un client SFTP et d'une paire de clés SSH que vous générerez vous-même.
Vous être libre du choix du client. Nous mettons à votre disposition deux des clients les plus courants (PuTTY et FileZilla) ainsi que leurs options de connexion.

1.6 Termes et abréviations

Abréviation	Définition
DMZ	DMZ signifie zone démilitarisée. Une DMZ est raccordée à une connexion LAN, un pare-feu entre un réseau interne et un réseau non sécurisé (par ex. Internet). Dans la DMZ, se trouvent fréquemment des serveurs fournissant des services pour les utilisateurs d'Internet (p. ex. www ou messagerie). Dans l'idéal, une DMZ se trouve entre deux pare-feux physiquement séparés. Le pare-feu externe protège des attaques de l'extérieur et contrôle chaque accès Internet à la DMZ. Le pare-feu interne contrôle l'accès en-dehors de la DMZ vers le réseau interne et inversement. Il représente ainsi une deuxième ligne de défense, au cas où le pare-feu externe céderait aux attaques. Ceci présente l'avantage de protéger aussi le réseau interne si un intrus devait atteindre le serveur web.
DNS	Le Domain Name System (DNS) est l'un des services les plus importants sur Internet. Sa tâche principale est de router les adresses internet vers l'adresse IP correspondante.
De bout en bout	Par bout en bout, on entend le lien entre une application de la PostFinance SA et l'application du client externe.
FileZilla	FileZilla est un client FTP. Avec lui, les données sont transmises via le serveur FTP – simplement via FTP ou cryptées via FTPS ou SFTP et par connexion SSL ou SSH.
FTP	Le File Transfer Protocol (FTP) est un protocole réseau spécifié dans le RFC 959 de 1985 pour la transmission de fichiers sur les réseaux TCP/IP. Il s'agit d'un protocole qui permet d'échanger des données entre différents ordinateurs – indépendamment de leurs systèmes d'exploitation et de l'endroit où ils se trouvent.
GSLB	Le Global Server Load Balancing (GSLB) sert principalement à la répartition des accès via une adresse d'accès aux centres de calcul éloignés géographiquement. La technologie GSLB travaille sur les mêmes bases générales que l'équilibrage de charge DNS.
IPSS	LAN Interconnect over IPSS est une prestation Swisscom. Swisscom peut interconnecter des réseaux locaux en une unique infrastructure de communication pour toute une entreprise. IPSS est une solution Swisscom dotée de la technologie la plus moderne. La technologie MPLS (Multi Protocol Label Switching) utilisée pour IPSS permet une grande flexibilité en ce qui concerne la bande passante. Le service est assuré par la Swisscom Enterprise Solution. Plus d'informations sur: http://www.swisscom.com/es/
MAC	MAC (Message Authentification Code) est un système de cryptographie qui se base sur des clés symétriques ayant pour but de garantir l'intégrité des messages.
MFTPF	Managed File Transfer PostFinance (MFTPF) est un service qui contient la réception et l'expédition de fichiers de et vers PostFinance.
MPLS	Multi Protocol Label Switching (MPLS) est une implémentation du Label Switching. De telles procédures déchargent fortement les routeurs impliqués dans le transport d'un pack de données, le niveau de complexités se réduisant à celui d'un commutateur. Cette réduction est obtenue en établissant un chemin fixe au début de la transmission des données. Les routeurs sur cet itinéraire ne sont plus tenus d'examiner les packs de données à transmettre, mais ils se contentent de conduire ceux-ci sur le chemin activé auparavant.
Chiffrement public key	Le chiffrement public key est une procédure de cryptage asymétrique constituée d'une clé publique (Public) et d'une clé privée (Private). Toutes les utilisatrices et tous les utilisateurs génèrent leur propre paire de clés constituée d'une partie confidentielle (clé privée) et d'une partie non confidentielle (clé publique).
PuTTY	PuTTY est un client SSH gratuit pour Microsoft Windows.
SCP	SCP est un protocole de transfert crypté de données entre deux ordinateurs sur un réseau d'ordinateurs.
SFTP	SFTP File Transfer Protocol (SFTP) qu'on appelle également SSH File Transfer Protocol est un perfectionnement du protocole SCP permettant à un ordinateur client de transférer ses données de manière sûre sur des systèmes distants et d'accéder en toute sécurité aux fichiers qui s'y trouvent. Le protocole ne contient ni l'authentification ni le cryptage. Ces fonctions doivent être prises en charge par le protocole SSH qui y est subordonné. Il ne faut pas confondre SFTP avec Secure FTP ou avec FTP via SSL.
SSH	Secure Shell (SSH) désigne à la fois un protocole réseau et les programmes correspondants avec lesquels l'on peut établir une connexion réseau cryptée sur un ordinateur à distance de manière sûre.
Paire de clés SSH	Une paire de clés est constituée d'une partie confidentielle (clé privée) et d'une partie non confidentielle (clé publique).
TTL	Le Time to Live (TTL, en français Durée de vie) est la durée de validité des données dans les réseaux d'ordinateurs.
WinSCP	WinSCP est un logiciel SFTP et client FTP gratuit pour Windows. WinSCP copie des données entre les ordinateurs locaux et ceux à distance par le biais de divers protocoles: FTP, FTPS, SCP, SFTP et WebDAV.

2. Le Managed File Transfer PostFinance (MFTPF)

2.1 Vue d'ensemble

Le Managed File Transfer PostFinance (MFTPF) est le canal destiné au transfert de fichiers entre PostFinance et ses clientes et clients ainsi que ses partenaires. Le MFTPF remplace dès maintenant le produit FDS chez PostFinance.

2.2 Mise en place

MFTPF est composé de plusieurs serveurs d'applications, de banques de données et de périmètres. Tous ces composants se situent dans des zones différentes. Les serveurs de transfert de fichiers et de bases de données sont situés dans une zone hautement protégée, dont l'accès est strictement limité. Les serveurs de fichiers avec accès externe, que nous désignons par le terme de serveurs Secure-Transport-Edge sont situés dans des zones de protection moindre, auxquelles les clients peuvent accéder (DMZ). Les connexions client/serveur depuis les réseaux externes se font toujours via les serveurs Secure-Transport-Edge.

MFTPF est conçu sur le principe de la géo-redondance. Il est toujours disponible même en cas de défaillance d'un centre de calcul.

2.3 Branchement

2.3.1 Secure File Transfer Protocol (SFTP)

Seul SFTP est utilisé pour le transfert de fichiers entre PostFinance et ses clientes et clients / partenaires. SFTP (SSH Secure File Transfer Protocol) est un protocole de transfert de fichiers sécurisé. Une connexion cryptée de bout en bout est établie entre le client et le serveur, rendant les données et noms d'utilisateurs illisibles en cas de piratage. L'authentification s'effectue au moyen du chiffrement public key. Ainsi, le client peut se connecter sur le serveur sans interaction de l'utilisateur.
SSH garantit la transmission complète et inchangée des données de l'expéditeur au destinataire.

MFTPF supporte SSH-2 (version 2).

Attention: il ne faut pas confondre SFTP et FTPS (FTP via SSL) ou FTP via SSH!

2.3.2 Clients recommandés

PostFinance recommande les clients les plus courants WinSCP et FileZilla.
La configuration est révélée dans le chapitre 4.

2.3.3 Types de raccordement

Le transfert de fichiers passe généralement par Internet.

2.4 Réception et livraison des données

Différents répertoires sont mis à la disposition des clients et des clients sur le serveur MFTPF pour la réception et la livraison des données.
La livraison et la distribution d'un fichier se déroule en fonction des événements. Après la réception d'un fichier, celui-ci est transféré par le serveur MFTPF vers les destinations prédéfinies. Il est impossible de déterminer le moment précis de l'exécution d'une action.

Il est possible de connecter par PostFinance la réception et la livraison de fichier à un système cible externe (serveur client). Voici les prérequis du côté du client afin d'assurer un bon fonctionnement:
- L'infrastructure et le centre de calcul sont disponibles 24h/24 et 7j/7.
- Les points de contact pour assistance (numéros de téléphone, e-mails) sont joignables 24h/24 et 7j/7.

3. Paramètres de configuration

Le chapitre qui suit offre une vue d'ensemble des paramètres de configuration.

3.1 Prérequis SFTP

Le serveur MFTPF supporte:
- Version 2: protocole SSH
- Version 3: protocole SFTP
- Commandes entrantes SCP avec protocole SSH/SCP (Attention: SCP ne possède pas les commandes *list, rename* et *delete*)
- Algorythmes de cryptage: AES avec une longueur de clé de 128 bits min.
- Message Codes d'authentification (MAC): hmac-sha2-256
- Transferts de données d'une taille maximale de 50 Go
- Cinquante connexions simultanées depuis le même compte
- Fermeture du compte après 3 échecs de connexion
- Les clés sont supportées dans les formats OpenSSH, ssh.com et PuTTY
- Une ou plusieurs clés peuvent être configurées pour chaque compte

3.2 Nom de l'hôte, port et adresses IP

Environnement	Nom de l'hôte	Port
Production	mftp1.postfinance.ch	8022

La répartition de la communication par l'intermédiaire de deux sites est obtenue à l'aide d'un DNS de répartition de charge (round-robin). Cela signifie que les adresses IP des deux sites sont retournées par alternance.

Il faut s'assurer que la communication vers et depuis MFTPF est autorisée dans votre réseau. Dans de nombreux cas, l'équipe en charge du réseau doit autoriser les connexions avec les règles de pare-feu correspondantes. Deux adresses IP sont utilisées. Les adresses IP ne doivent être utilisées que pour la configuration de règles de pare-feu. Pour établir une connexion, il faut obligatoirement utiliser le nom DNS.

Les deux adresses IP peuvent être déterminées au moyen de plusieurs tentatives par résolution DNS (nslookup mftp1.postfinance.ch). MFTPF supporte IPv4 et IPv6. L'utilisation d'IPv6 implique le support en continu IPv6 dans votre infrastructure.

3.3 Cache DNS

La plateforme est exploitée sur deux sites dans une configuration active/active. Le mécanisme de basculement est assuré par une infrastructure *Global Server Load Balancing (GSLB)*. Afin de profiter d'un basculement rapide de la connexion au MFTPF, il faut vous assurer qu'aucun autre cache DNS n'est fait dans votre environnement. Les indications relatives au «Time to live» (TTL) du DNS de PostFinance doivent être impérativement respectées.

3.4 Autorisation

Pour se connecter au serveur MFTPF, il faut un nom d'utilisateur (MFTPF User ID) et une clé SSH valide.

Noms d'utilisateur (MFTPF User ID)
Le nom d'utilisateur est communiqué dans le cadre de la commande du canal MFTPF.

Clé publique
La clé SSH doit avoir une longueur minimale de 4096 bits. Le système de cryptographie utilisé est RSA.

Si on le souhaite, il est possible de configurer plusieurs clés publiques pour le même nom d'utilisateur. Inversement, plusieurs utilisatrices et utilisateurs peuvent se servir de la même clé.

Conformément à la demande d'adhésion, une copie de la clé publique doit être envoyée à PostFinance.

3.5 Répertoires

Les répertoires sont créés par PostFinance. Les utilisatrices et les utilisateurs ne peuvent ni créer les répertoires, ni les effacer.

La syntaxe des répertoires contient les caractères suivants:
– Caractères: [a–z], [0–9], [. -] (point, trait d'union)
– Début: le premier caractère doit être [a–z], [0–9]

Nous porterons à votre connaissance les répertoires qui vous concernent au moment de l'adhésion au canal.

3.6 Noms de fichiers

Pour les noms de fichiers, les caractères suivants peuvent être utilisés:
– Caractères: [A–Z], [a–z], [0–9], [. - _] (point, trait d'union, tiret bas)

Les noms de fichiers transmis par PostFinance, varient en fonction des prestations et tiennent cependant compte de la syntaxe décrite précédemment. Veillez impérativement à ce que les fichiers que vous créez, contiennent bien cette syntaxe. C'est la seule manière pour nous de garantir le traitement des fichiers.

4. Créer les clés SSH et générer le client

Le présent chapitre décrit comment générer les clés SSH avec PuTTY et OpenSSH et comment configurer les clients les plus courants FileZilla et WinSCP pour le transfert de fichiers.

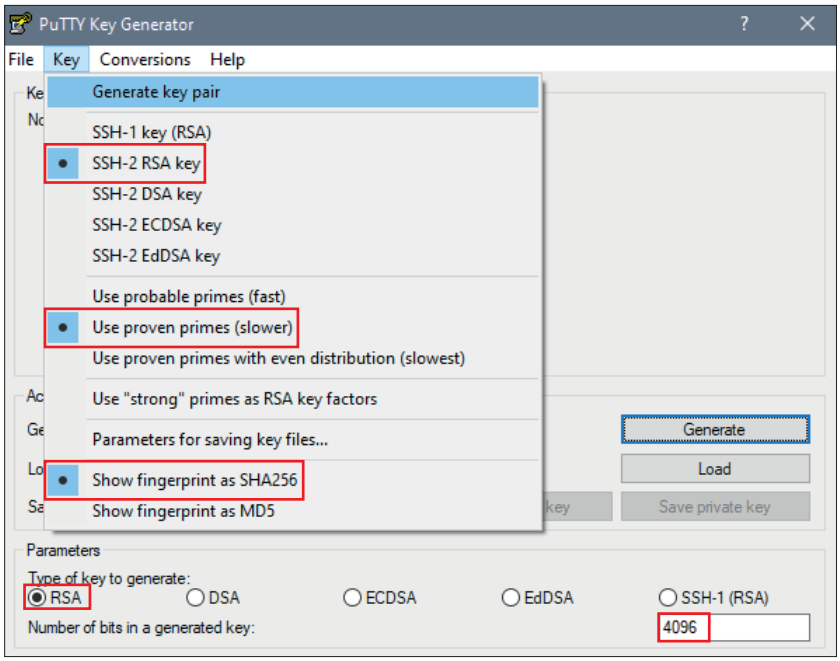
4.1 Créer une paire de clés SSH avec PuTTY

PuTTY est un logiciel open source pour Microsoft Windows. Il est téléchargeable sur http://www.putty.org.
La clé privée et la clé publique peuvent être générées séparément avec le client SSH/SFTP (putty.exe). Il existe la possibilité de générer des paires de clés avec PUTTYgen.

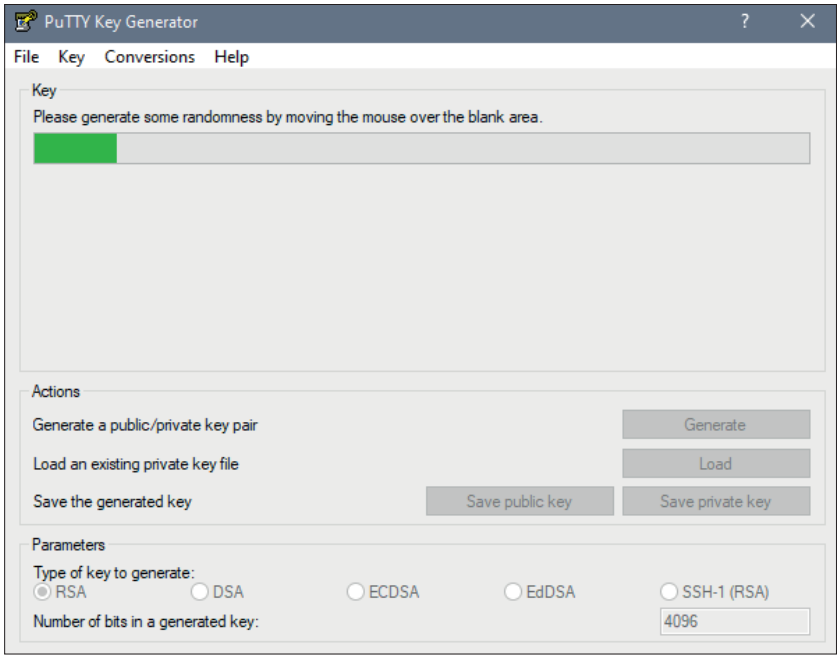
Lancer PuTTYgen

Choisir *SSH-2 RSA* comme type de clé.
Saisir une longueur de *4096* bits.

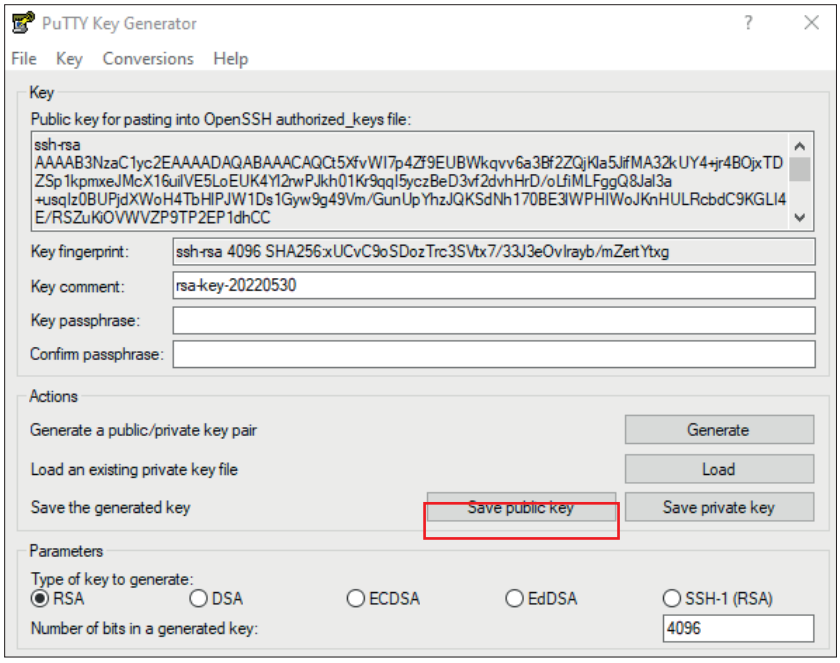
Cliquer sur *Generate*.



Se rendre sur la zone en dessous de la barre verte à l'aide du curseur.



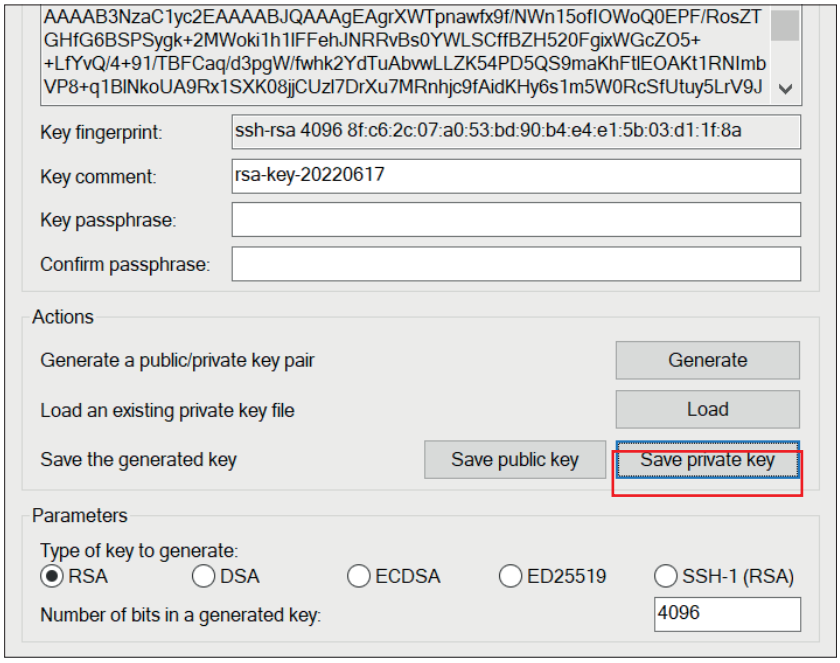
Le masque avec les clés apparaît sitôt la clé générée.
Sélectionner *Save public key.*



Sélectionner *Save private key.*

Attention: la clé privée doit être sauvegardée sur votre système informatique, protégée des accès non autorisés et ne doit JAMAIS être transmise à quiconque.

Pour que la clé privée soit protégée contre une utilisation abusive, il est conseillé de la générer avec une phrase clé. Il faut toutefois garder à l'esprit que selon le logiciel utilisé, une automatisation de l'adhésion peut devenir plus difficile.



4.2 Créer une paire de clés SSH avec OpenSSH

OpenSSH est disponible en version packagée sur toutes les plateformes UNIX. Des informations complémentaires peuvent être consultées sous http://www.openssh.com.

La paire de clés SSH peut être générée avec la commande suivante:

```
ssh-keygen -b 4096 -t rsa -f /tmp/demo_key -C
„Commentaire pour Demo Key"
```

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-----
```

Voici un exemple de clé publique (celle-ci est générée automatiquement avec le suffixe .pub):

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

4.3 Envoyer la clé publique à PostFinance

Une copie de la clé publique doit être transmise à PostFinance.

Prestation	Adresse e-mail
Trafic des paiements	tscorp@postfinance.ch
Reconciliation Files/RAF	aqs@postfinance.ch
Autres	mftpf@postfinance.ch

Afin que PostFinance puisse vérifier avec l'expéditrice ou l'expéditeur la clé transmise, il faut que la personne de contact envoie la clé (ou que la clé apparaisse dans un échange mails). Après obtention de la clé publique, un collaborateur ou une collaboratrice de PostFinance se mettra en relation avec la personne de contact afin de synchroniser les derniers chiffres de la valeur hash générée par SHA256 de la clé publique. On s'assure ainsi qu'aucune manipulation par un tiers n'aura lieu.

Dès que nous avons installé la clé, nous vous signalons la fin de la procédure. Vous pouvez alors tester la connexion.

Traitez votre clé privée comme votre propre carte de crédit! Protégez-la des accès non autorisés.

4.4 Tester la connexion

Pour le test de connexion, veuillez sélectionner le nom de l'hôte souhaité pour l'environnement de production et de test (voir chapitre 3.2 *Nom de l'hôte, port et adresses IP*).

Dans le cadre de la commande de services, le nom d'utilisateur ainsi que les détails relatifs aux noms du répertoire et noms de fichiers seront communiqués.

4.4.1 Test de la connexion avec Telnet

La connexion à MFTPF peut être par exemple testée avec Telnet:

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

Attention: deux adresses IP sont utilisées. Les deux adresses IP peuvent être déterminées au moyen de plusieurs tentatives par résolution DNS (nslookup mftp1.postfinance.ch ou mftt1.postfinance.ch). Les adresses IP ne doivent être utilisées que pour la configuration de règles de pare-feu. Pour établir une connexion, il faut obligatoirement utiliser le nom DNS.

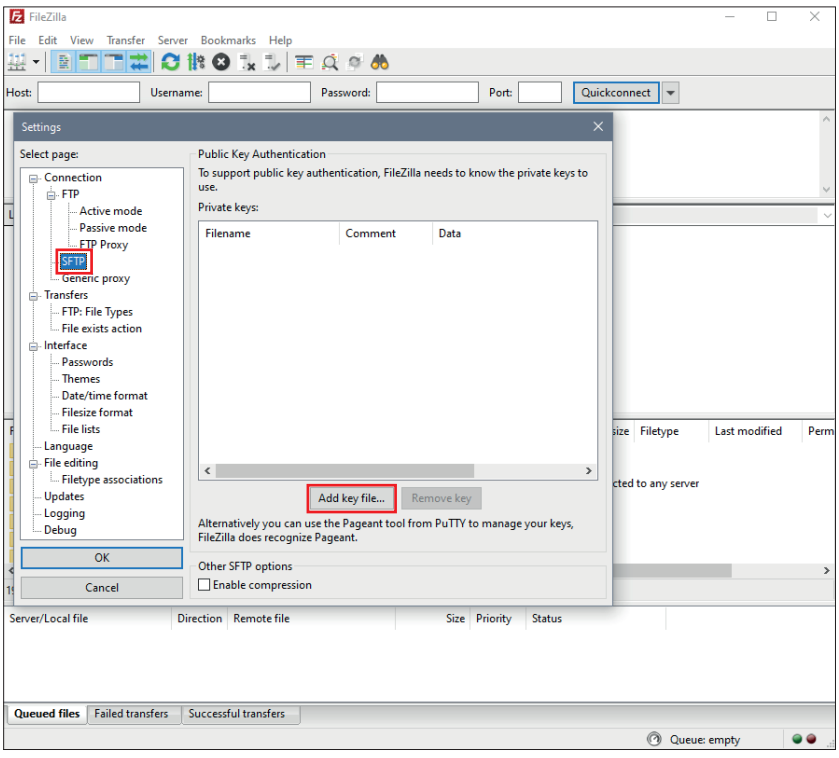
4.5 Configuration FileZilla

4.5.1 Importer une clé avec FileZilla

Pour l'import, il est possible de créer une clé avec PuTTY ou OpenSSH.

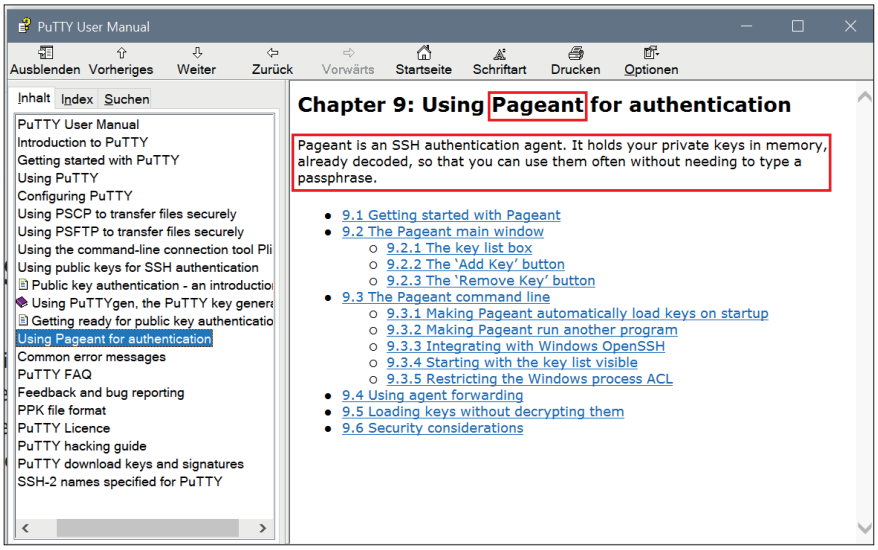
Lancer FileZilla.
Sélectionner *Édition* et ensuite *Paramètres*.
Sélectionner la page: *SFTP*
Sélectionner *Ajouter clé*.

Ajouter la clé privée générée auparavant.

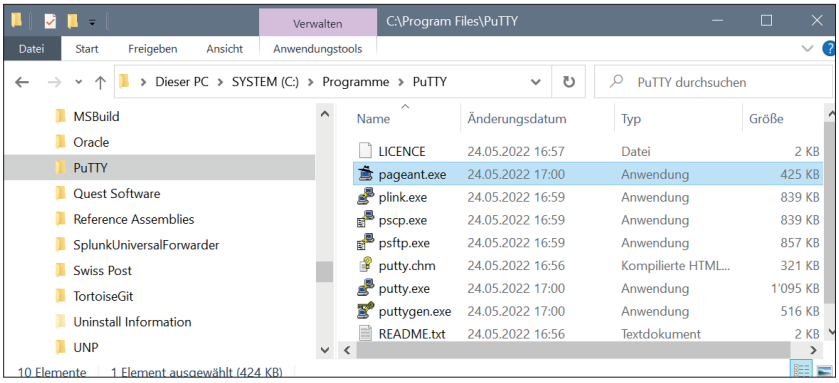


4.5.2 Importation automatique avec PuTTY's Pageant

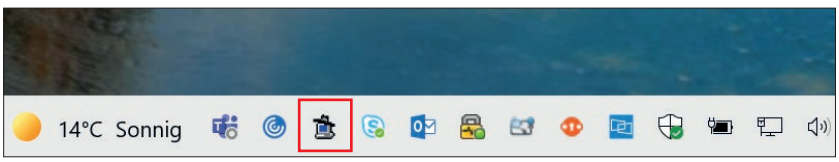
Attention: il faut générer la clé avec PuTTY pour utiliser PuTTY's Pageant.
Le *Pageant* (agent d'authentification PuTTY) est un agent SSH, par le biais duquel les authentifications SSH peuvent être transmises. Pageant peut charger des clés et les mettre sur demande à disposition de programmes locaux. L'interface est ouverte, de manière à ce que d'autres programmes puissent se connecter à ce service de Pageant.



Lancer Pageant.exe.

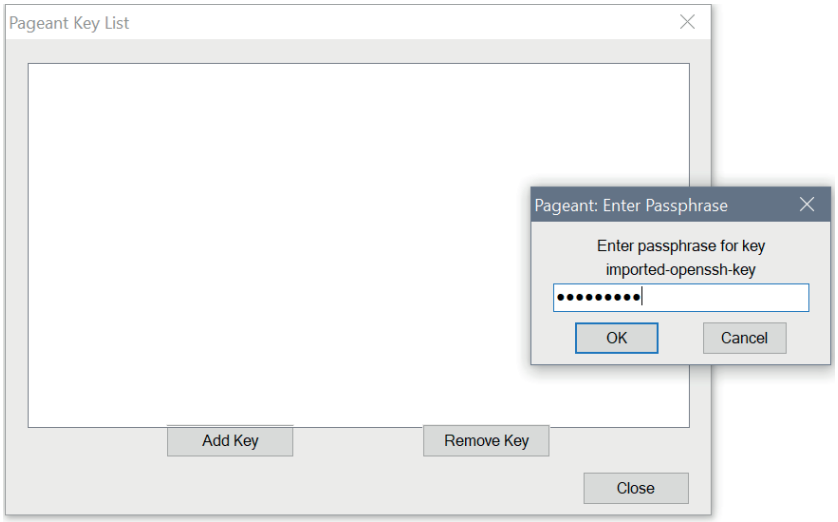


Pageant se trouve dans la barre d'état système en bas à droite dans la barre de démarrage rapide et affiche toutes les sessions sauvegardées dans Pageant.



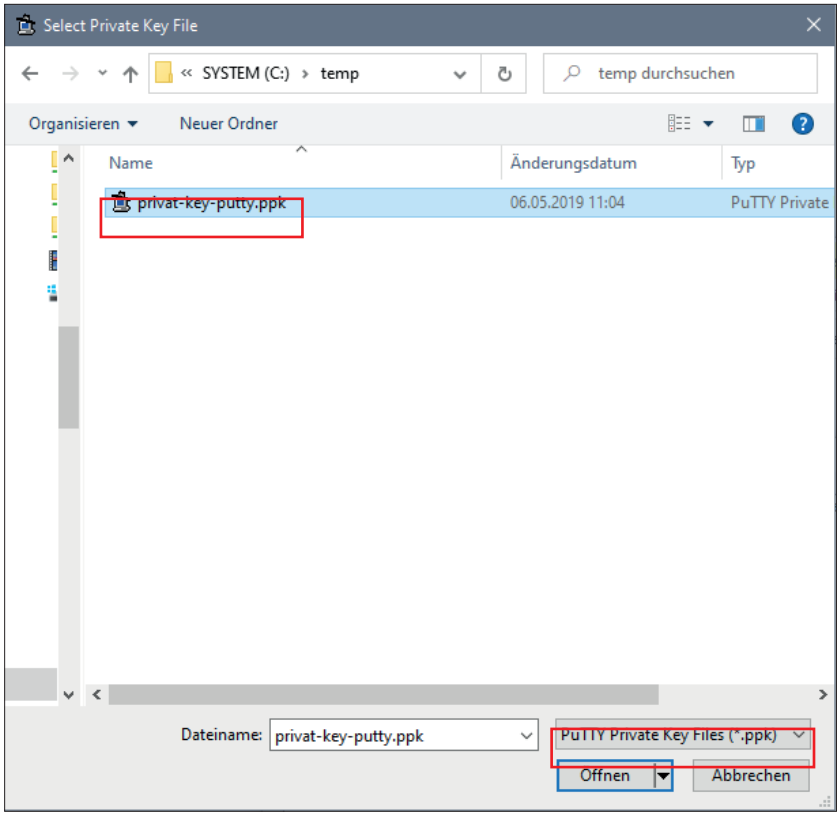
Double-clic sur l'icône «chapeau».

Pour sélectionner la clé privée, ouvrir la fenêtre en cliquant sur *Add Key*.

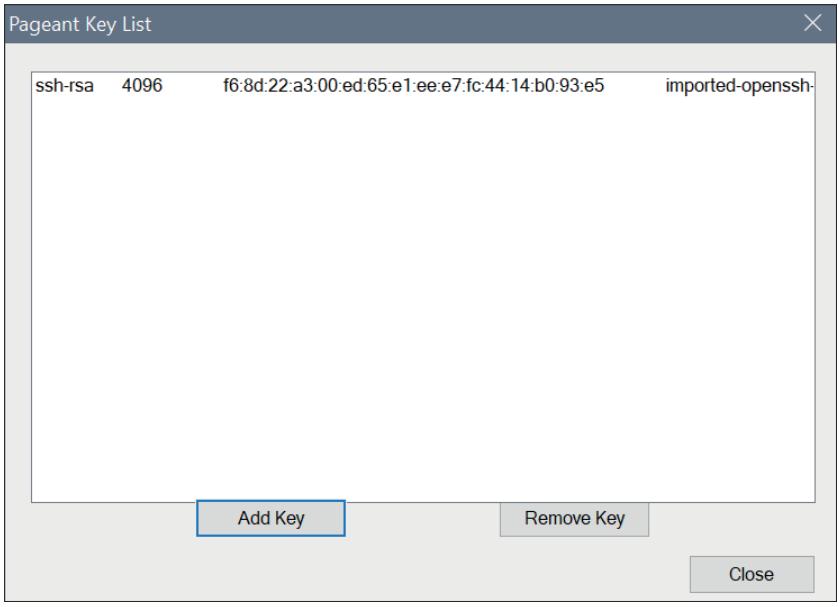


Sélectionner la clé privée et confirmer avec *Ouvrir*.

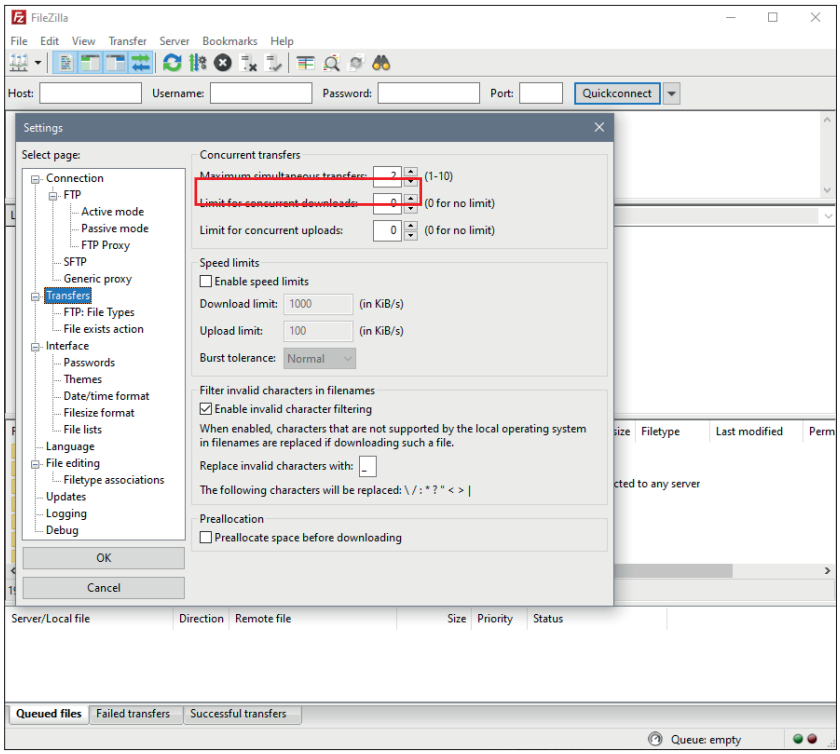
Attention: seules les clés générées avec PuTTY peuvent être prises en charge.



La clé importée correctement devrait ressembler à l'exemple ci-contre.



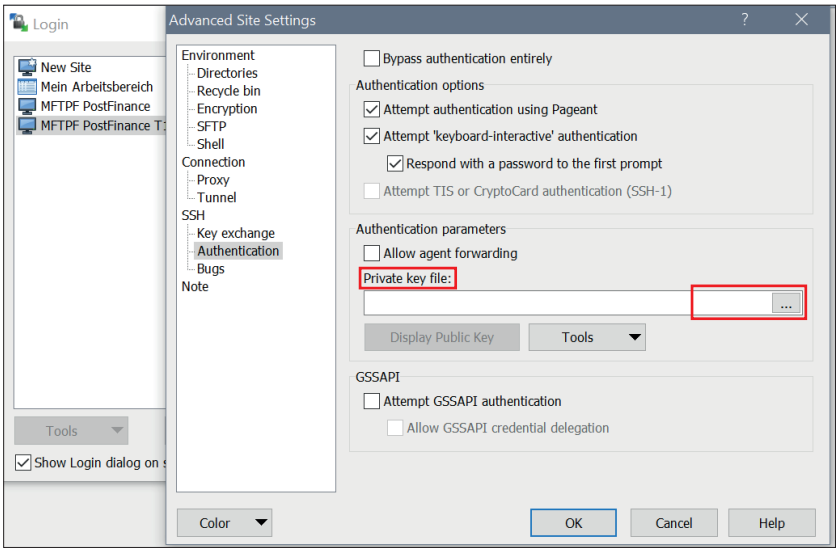
Remarque:
Afin d'éviter un lock-out, nous recommandons de limiter le nombre de transmissions simultanées à *trois*.



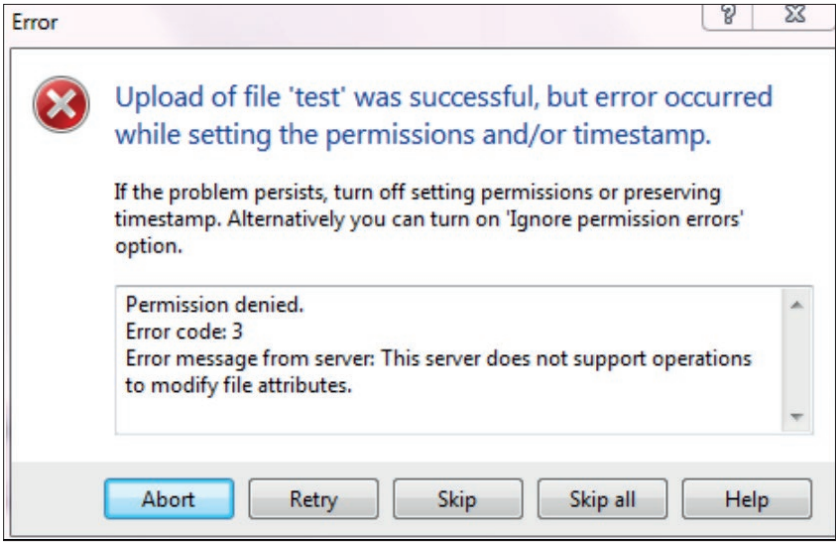
4.6 Configuration WinSCP

4.6.1 Importer une clé avec WinSCP

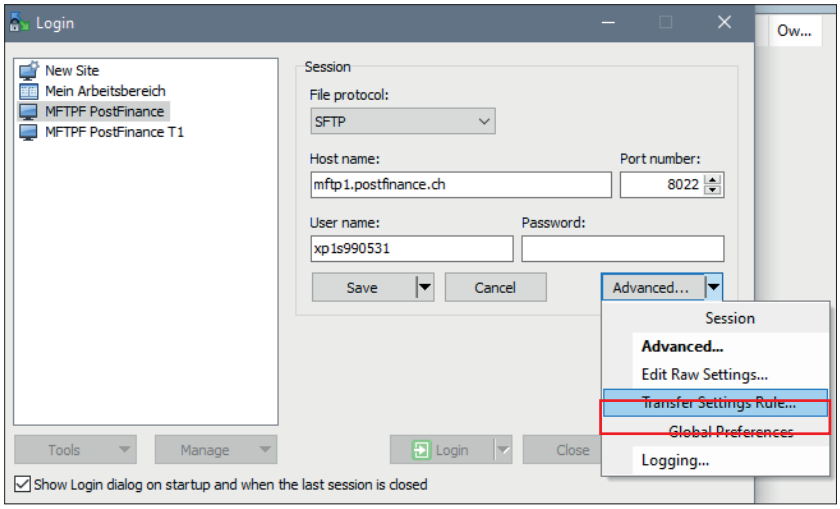
Lancer WinSCP.
Élargi
Authentification
Sous *Fichier avec clé privée* […]
cliquer et sélectionner la clé privée.



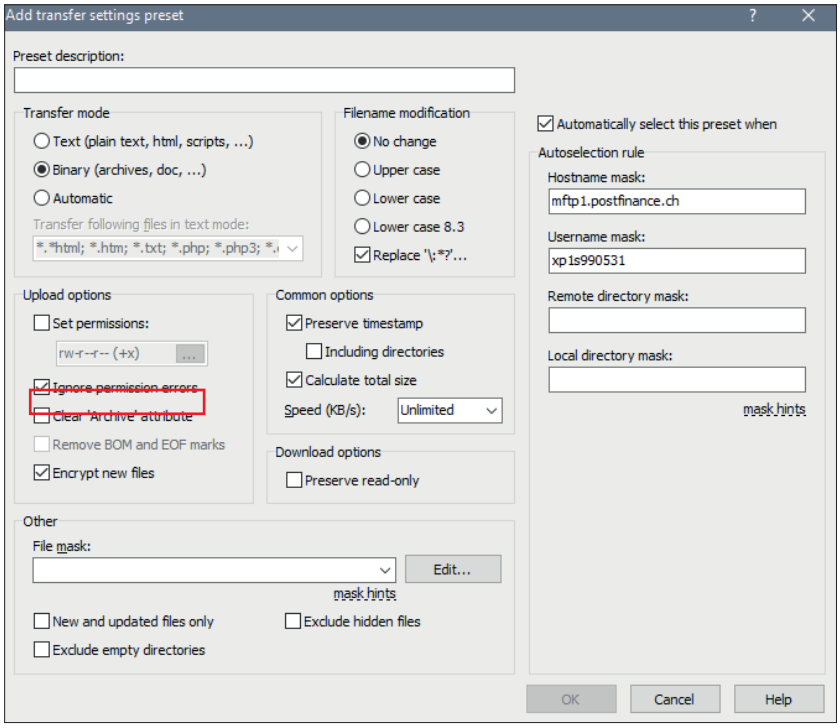
Les problèmes d'authentification après le téléchargement comme indiqué dans la capture d'écran ci-contre, peuvent être résolus en modifiant les paramètres.



Rendez-vous sur
Élargi
Règles des paramétrages de transfert
Et sélectionnez celles-ci.



Activez
ignorer les erreurs d'authentification



5. Informations sur l'utilisation MFTPF

Cette information brève décrit l'échange de données ainsi que les fonctions de MFTPF et énonce les règles et directives à caractère général concernant le transfert de données avec les serveurs MFTPF.

5.1 Conditions-cadres/Restrictions

a) MFTPF n'est pas un système d'archivage. Les données à récupérer que la cliente ou le client n'a pas encore effacées, sont en tous les cas supprimées automatiquement par le serveur au bout de neuf jours.
b) Pour transmettre un grand nombre de fichiers, on effectuera un nombre proportionnel de transferts (put/get) par session SFTP. Exemple pour 1200 fichiers: 10 liaisons/logins FTP de 120 transferts de fichiers. Si un nombre trop élevé de logins est effectué pendant une unité de temps donnée, le système de prévention d'intrusion de PostFinance bloque automatiquement pendant 15 minutes l'adresse IP source en cause.
c) MFTPF ne confirme pas le transfert aux expéditrices et expéditeurs, c'est-à-dire que MFTPF ne leur envoie pas de message de réception à la livraison des fichiers. La création et l'envoi de confirmation (par ex. en cas de livraison de messages pain.001, vous trouverez des messages pain.002) relèvent des systèmes récepteurs et ne sont pas assurés par MFTPF.
d) En cas de retransmission à d'autres destinataires, l'ordre des fichiers transférés n'est pas garanti. Des fichiers de taille variable peuvent se dépasser par une transmission de données parallèle. Il appartient au système de réception de la relation de bout en bout de rétablir l'ordre correct des fichiers transmis.
e) La transmission et la distribution de fichiers est commandée selon les événements. Une gestion temporelle est impossible.

Restrictions en cas de livraison de fichiers (client → serveur MFTPF)
- Si un client de transfert de fichiers exécute une fonction de livraison (put) dans un répertoire MFTPF, les fichiers seront traités par les processus sur le serveur MFTPF par les processus sitôt le transfert terminé. Les entrées des fichiers dans les boîtes de téléchargement restent cependant visibles pour les clientes et le clients pendant 2 minutes (affichage des fichiers par «dir» et «ls»). La suppression ou le changement de nom d'un fichier envoyé est sans effet: celui-ci sera toujours retransmis au/à la destinataire avec son nom initial.
- MFTPF s'assure que seuls les fichiers transmis intégralement seront traités. En cas d'échec de la connexion, le fichier incomplet sera rejeté.
- Une modification des attributs du fichier après le transfert sur MFTPF est impossible.