Manuale
Managed File Transfer PostFinance (MFTPF)

PostFinance

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

Supporto clienti

In caso di domande sui prodotti PostFinance e sui canali del traffico dei pagamenti, la clientela può rivolgersi alla o al consulente clienti personale.

In alternativa è possibile rivolgersi alla **Consulenza Clienti commerciali:**
Consulenza e vendita
Telefono +41 848 888 900
(in Svizzera max CHF 0.08/min)

Colophon
PostFinance SA
3030 Berna

Versione
Maggio 2023

Indice

1. Informazioni generali

1.1 Gruppo target del canale Managed File Transfer PostFinance (MFTPF)

PostFinance SA offre alla sua clientela diversi canali per la trasmissione e la consegna di dati. Il canale Managed File Transfer PostFinance (MFTPF) consente un trasferimento dei dati sicuro e automatizzato tra la clientela e PostFinance per uno svolgimento efficiente del traffico dei pagamenti e, in generale, per lo scambio di dati. Questo servizio si rivolge alla clientela commerciale che scambia regolarmente dati (dati per il traffico dei pagamenti, Reconciliation Files / RAF, software ecc.) con PostFinance tramite un canale sicuro.

1.2 Uso del manuale

Il presente manuale spiega come avviene lo scambio di file con il server MFTPF di PostFinance SA e si rivolge ai responsabili IT che si occupano di allestire il collegamento tra il server del/della cliente e quello MFTPF presso PostFinance.
La prima parte del manuale illustra il funzionamento del server MFTPF. La seconda riporta i parametri di configurazione necessari nonché una descrizione su come allestire i client SFTP più comuni e generare la coppia di chiavi SSH.

1.3 Disposizioni applicabili e manuali

A meno che il manuale Managed File Transfer PostFinance (MFTPF) non contenga disposizioni particolari, si applicano le Condizioni generali di PostFinance SA e le Condizioni di adesione Offerta di servizi digitali.
Il presente manuale e le Condizioni generali e condizioni di adesione di PostFinance possono essere scaricati all'indirizzo www.postfinance.ch/manuali.

1.4 Adesione

L'adesione al canale MFTPF avviene tramite il vostro o la vostra consulente clienti o il Customer Center.

1.5 Come utilizzare il canale MFTPF

Dopo aver esaminato e approvato l'adesione, vi inviamo il vostro User ID MFTPF.

Vi servono inoltre un client SFTP e una coppia di chiavi SSH che potete creare in autonomia.
Potete scegliere liberamente il client. In questo manuale vi presentiamo i due più comuni (PuTTY e FileZilla) e le rispettive possibilità di collegamento.

1.6 Termini e abbreviazioni

Abbreviazione	Definizione
DMZ	DMZ sta per Demilitarized Zone (zona demilitarizzata). Una DMZ si trova in una connessione LAN separata di un firewall tra una rete interna e una rete esterna non sicura (ad es. internet). Nella DMZ vengono spesso messi a disposizione server che offrono servizi agli utenti di internet (ad es. www o e-mail). Una DMZ si trova di preferenza tra due firewall separati fisicamente. Il firewall esterno protegge dagli attacchi dall'esterno e controlla ogni accesso internet alla DMZ. Il firewall interno controlla l'accesso dalla DMZ alla rete interna e viceversa. Costituisce così una seconda linea di difesa nel caso in cui il firewall esterno dovesse essere violato. Ciò presenta il vantaggio di proteggere la rete interna anche nel caso che un'aggressione raggiunga il server Web.
DNS	Il Domain Name System (DNS) è uno dei servizi più importanti in internet. Il suo compito principale è quello di commutare gli «indirizzi internet» nei relativi indirizzi IP.
End-to-end	L'end-to-end è la relazione tra un'applicazione di PostFinance SA e una del cliente esterno / della cliente esterna.
FileZilla	FileZilla è un client FTP. Consente di trasmettere dati tramite server FTP, in modo semplice tramite FTP o in modo criptato tramite FTPS o SFTP e via SSL o SSH.
FTP	Il File Transfer Protocol (FTP) è un protocollo di rete specificato nell'RFC 959 del 1985 per la trasmissione dei file attraverso le reti TCP/IP. È un protocollo che consente lo scambio di file tra computer diversi, indipendentemente dalla loro ubicazione e dal sistema operativo.
GSLB	Il Global Server Load Balancing (GSLB) serve soprattutto a distribuire gli accessi a centri di calcolo geograficamente distanti mediante un indirizzo di accesso centrale. La tecnologia GSLB funziona secondo gli stessi principi generali del bilanciamento del carico DNS.
IPSS	LAN Interconnect over IPSS è un servizio di Swisscom, che riesce a collegare reti locali a un'unica infrastruttura di comunicazione aziendale. IPSS è una soluzione propria di Swisscom dotata della tecnologia più moderna. La tecnologia MPLS (Multi Protocol Label Switching) utilizzata consente una grande flessibilità in termini di larghezza di banda. Il servizio è integralmente assicurato da Swisscom Enterprise Solution. Maggiori informazioni: http://www.swisscom.com/es/
MAC	MAC (Message Authentification Code) è un sistema di crittografia basato su chiavi simmetriche che punta a garantire l'integrità dei messaggi.
MFTPF	Managed File Transfer PostFinance (MFTPF) è un servizio che comprende la ricezione e l'invio di file da e verso PostFinance.
MPLS	Il Multi Protocol Label Switching (MPLS) è un'implementazione del Label Switching. In questo processo si riduce il carico dei router utilizzati per il trasporto dei pacchetti dati, poiché il livello di complessità del processo è ridotto a un semplice switch. Ciò è possibile perché all'inizio della trasmissione dei dati viene creato un percorso di connessione fisso. I router su questo percorso non devono individuare il destinatario dei pacchetti in transito, ma li trasferiscono senza elaborazioni secondo il percorso impostato.
Procedura public key	La procedura public key è una procedura di crittografia asimmetrica costituita da una chiave pubblica (public) e una privata (private). Ogni utente crea la propria coppia di chiavi, composta da una parte nascosta (chiave privata) e una non nascosta (chiave pubblica).
PuTTY	PuTTY è un client SSH libero per Microsoft Windows.
SCP	SCP è un protocollo per la trasmissione cifrata di dati tra due computer mediante una rete informatica.
SFTP	Il Secure File Transfer Protocol (SFTP), detto anche SSH File Transfer Protocol, è uno sviluppo ulteriore dell'SCP e permette la trasmissione di e l'accesso ai dati da un client su un sistema remoto in sicurezza. Il protocollo non include né l'autenticazione né la cifratura. Tali funzioni devono essere riprese dal protocollo SSH sottostante. Non confondere SFTP con Secure FTP o con FTP tramite SSL.
SSH	Secure Shell (SSH) indica sia un protocollo di rete sia i relativi programmi, grazie ai quali è possibile creare in modo sicuro un collegamento di rete cifrato con un computer remoto.
Coppia di chiavi SSH	Una coppia di chiavi composta da una parte nascosta (chiave privata) e una non nascosta (chiave pubblica).
TTL	Time to live (TTL, in italiano tempo di vita) è la durata di validità assegnata ai dati nelle reti informatiche.
WinSCP	WinSCP è un software client SFTP e FTP libero per Windows che copia i file tra computer locali e remoti con diversi protocolli: FTP, FTPS, SCP, SFTP e WebDAV.

2. Il Managed File Transfer PostFinance (MFTPF)

2.1 Panoramica

Il Managed File Transfer PostFinance (MFTPF) è il canale per trasferire file tra PostFinance e la sua clientela nonché i suoi partner. Sostituisce fin da subito il prodotto FDS presso PostFinance.

2.2 Struttura

MFTPF è composto da più server di applicazione, banca dati e perimetro. Tutti i componenti sono collocati in zone diverse. I server di trasferimento file e di banca dati si trovano all'interno di una zona altamente protetta e ad accesso estremamente limitato. I file server accessibili dall'esterno, che da noi sono chiamati Secure Transport Edge, si trovano in zone con una protezione inferiore, a cui è consentito accedere con i client (DMZ). I collegamenti client/server dalle reti esterne viaggiano sempre su server Secure Transport Edge.

MFTPF è geograficamente ridondante. Continuerà a essere disponibile anche in caso di eventuale guasto a un centro di calcolo.

2.3 Collegamento

2.3.1 Secure File Transfer Protocol (SFTP)

Per il trasferimento di file tra PostFinance e la clientela / i partner si usa esclusivamente SFTP (Secure File Transfer Protocol), che rappresenta un protocollo sicuro. Tra client e server viene infatti stabilito un collegamento ininterrotto e cifrato tramite il quale i nomi utente e i dati risultano illeggibili per eventuali intrusi. Per l'autenticazione si utilizza la procedura public key, in modo che il client possa eseguire il login al server senza l'interazione dell'utente.
L'SSH garantisce una trasmissione completa e integrale dei dati dal mittente al destinatario.

MFTPF supporta SSH-2 (versione 2).

Attenzione: l'SFTP non va confuso con l'FTPS (FTP mediante SSL) o con l'FTP mediante SSH!

2.3.2 Client raccomandati

PostFinance consiglia i client più comuni, ovvero WinSCP e FileZilla. La configurazione è illustrata al capitolo 4.

2.3.3 Tipi di connessione

Il trasferimento di file si svolge di norma tramite internet.

2.4 Trasmissione e consegna

Sul server MFTPF la clientela ha a disposizione diverse directory per la trasmissione e la consegna.
La consegna e la ripartizione di un file avvengono per evento. All'arrivo di un file, il server MFTPF lo invia alle destinazioni predefinite. Non è possibile stabilire quando un'azione debba essere eseguita.

Si possono trasmettere e consegnare file a un sistema di destinazione esterno (server cliente) attraverso PostFinance. Per garantire una gestione ottimale la clientela deve soddisfare i seguenti requisiti:
– infrastruttura e funzionamento del centro di calcolo disponibili 24/7
– uffici di contatto per il supporto (numeri di telefono, e-mail) reperibili 24/7

3. Parametri di configurazione

Il seguente capitolo fornisce una panoramica dei parametri di configurazione.

3.1 Requisiti SFTP

Il server MFTPF supporta
- versione 2: SSH Protocol
- versione 3: SFTP Protocol
- comandi SCP in ingresso con protocollo SSH/SCP (attenzione: SCP non supporta i comandi *list, rename* e *delete*)
- algoritmi di crittografia: AES con una lunghezza della chiave di almeno 128 bit
- Message Authentication Codes (MAC): hmac-sha2-256
- trasmissioni di file fino a un volume massimo di 50 gigabyte
- 50 collegamenti contemporanei dallo stesso account
- blocco dell'account dopo tre tentativi di login errati
- le chiavi supportate sono quelle in formato OpenSSH, ssh.com e PuTTY
- per ciascun account possono essere configurate una o più chiavi

3.2 Nome host, porta e indirizzi IP

Ambiente	Nome host	Porta
Produzione	mftp1.postfinance.ch	8022

La distribuzione della comunicazione sulle due sedi è realizzata con DNS Load Balancing (round-robin). Ciò significa che saranno restituiti alternativamente gli indirizzi IP delle due sedi.

Assicuratevi che la vostra rete permetta la comunicazione da o verso MFTPF. In molti casi il team di rete deve consentire la creazione dei collegamenti attraverso apposite regole del firewall. Si utilizzano due indirizzi IP che possono essere utilizzati solo per configurare le regole del firewall. Per allestire il collegamento è obbligatorio utilizzare il nome DNS.

Entrambi gli indirizzi IP possono essere determinati con risoluzione DNS (nslookup su mftp1.postfinance.ch) effettuando più tentativi.
MFTPF supporta IPv4 e IPv6. L'uso di IPv6 richiede un supporto completo di IPv6 nella vostra infrastruttura.

3.3 Caching DNS

La piattaforma viene gestita con una configurazione attiva/attiva tra due sedi. Il meccanismo di failover viene garantito con un'infrastruttura *Global Server Load Balancing (GSLB)*. Per poter usufruire di una connessione di failover rapida, dovete assicurarvi che nessuna cache DNS aggiuntiva sia configurata nella vostra rete. L'indicazione del time-to-live (TTL) del DNS di PostFinance deve essere rigorosamente rispettata.

3.4 Autorizzazione

Per collegarsi al server MFTPF sono necessari il nome utente (User ID MFTPF) e una coppia di chiavi SSH valida.

Nomi utente (User ID MFTPF)
Il nome utente viene comunicato in fase di ordinazione del canale MFTPF.

Public key
La chiave SSH deve avere una lunghezza di minimo 4096 bit. Il sistema di crittografia è RSA.

Volendo esiste la possibilità di configurare più public key per lo stesso nome utente. La stessa chiave può essere usata da più utenti.

Una copia della public key deve essere inviata a PostFinance secondo l'adesione.

3.5 Directory

Le directory sono create da PostFinance. L'utente non può né crearle né cancellarle.

La sintassi delle directory contiene i seguenti caratteri:
– caratteri: [a-z], [0-9], [. -] (punto, trattino)
– inizio: il primo carattere deve essere [a-z], [0-9]

Vi comunichiamo le directory rilevanti al momento dell'adesione al canale.

3.6 Nomi dei file

Per i nomi dei file vanno utilizzati i seguenti caratteri:
– caratteri: [A-Z], [a-z], [0-9], [. - _] (punto, trattino, trattino basso)

I nomi dei file forniti da PostFinance si distinguono in base al servizio, ma tengono conto della sintassi illustrata in precedenza.
Assicuratevi che i file creati rispettino rigorosamente questa sintassi.
Solo così potremo garantire la loro elaborazione.

4. Creare le chiavi SSH e allestire il client

Questo capitolo mostra come generare le chiavi SSH con PuTTY e OpenSSH e configurare i client più comuni per il trasferimento di file, ovvero FileZilla e WinSCP.

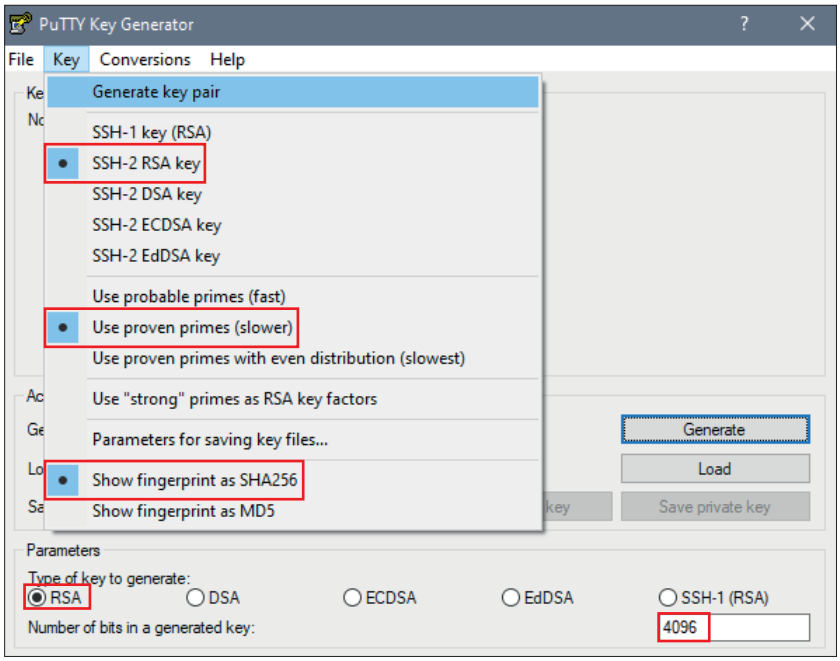
4.1 Creare una coppia di chiavi SSH con PuTTY

PuTTY è un software open source per Microsoft Windows. Può essere scaricato da http://www.putty.org.
Con il client SSH/SFTP (putty.exe) si possono generare separatamente private e public key. PuTTYgen consente di generare coppie di chiavi.

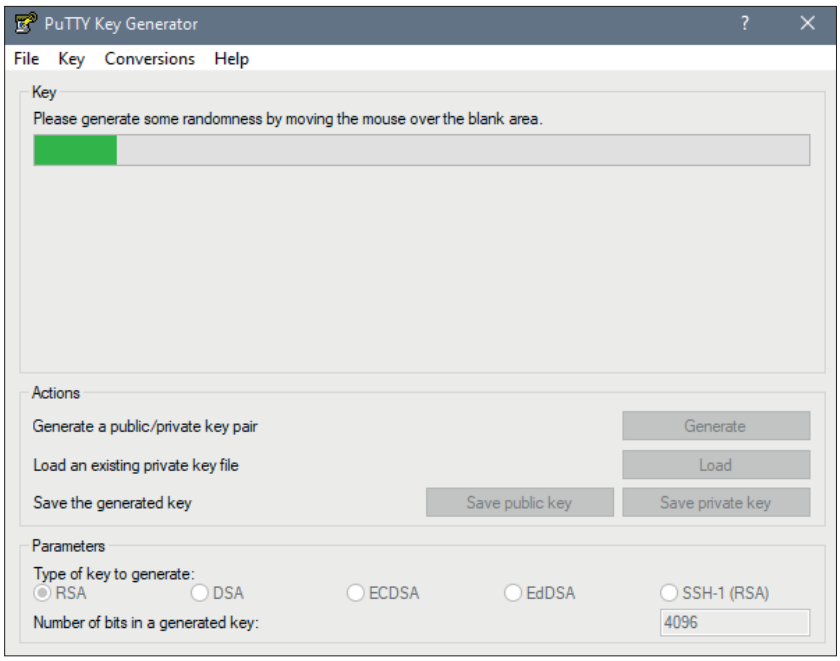
Avviare PuTTYgen.

Scegliere *SSH-2 RSA* come tipo di chiave.
Inserire *4096* bit come lunghezza.

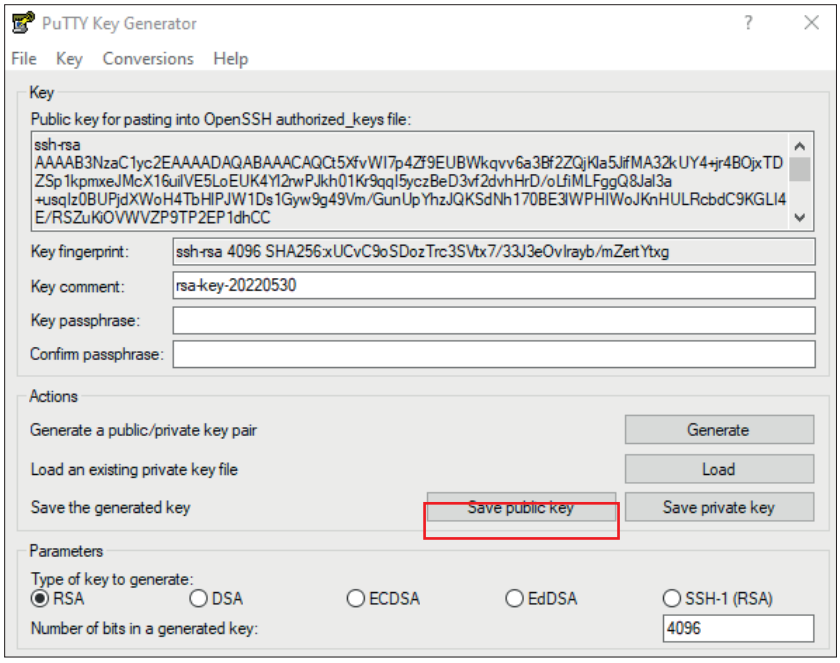
Fare clic su *Generate*.



Muovere il cursore del mouse sulla superficie sotto la barra verde.



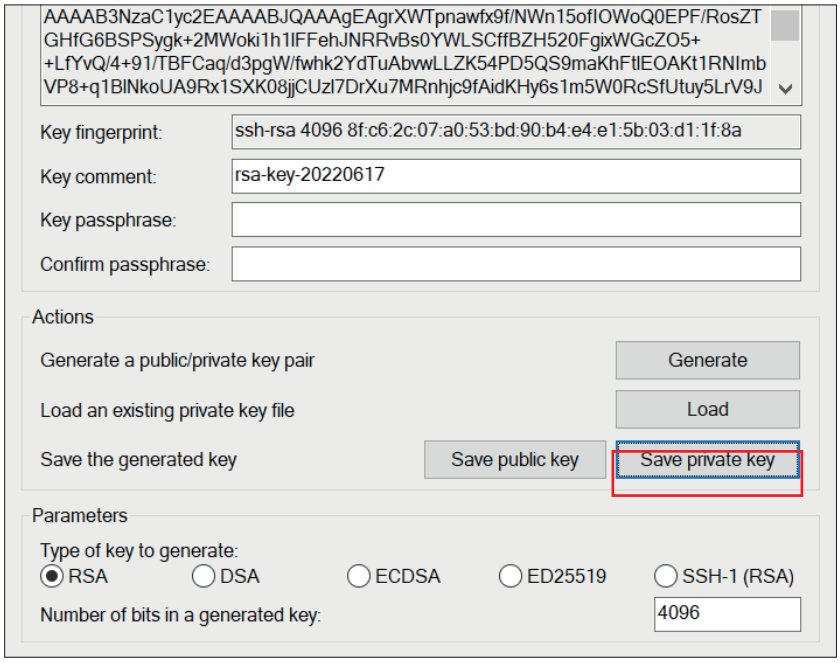
Una volta conclusa la generazione della chiave, compare la maschera con le chiavi.
Selezionare *Save public key*.



Selezionare *Save private key*.

Attenzione: la private key deve essere salvata sul vostro sistema IT, protetta contro gli accessi non autorizzati e non va MAI trasmessa a terzi.

Affinché la private key sia protetta dall'uso non autorizzato, consigliamo di generarla con una passphrase. Si deve però considerare che, a seconda del software utilizzato, l'automazione del login può così risultare più difficile.



4.2 Creazione di una coppia di chiavi SSH con OpenSSH

OpenSSH è disponibile come pacchetto di programma su tutte le piattaforme Unix. Per maggiori informazioni visitare http://www.openssh.com.

La coppia di chiavi SSH può essere generata con il seguente comando:

```
ssh-keygen -b 4096 -t rsa -f /tmp/demo_key -C
„Commento per chiave demo“
```

Ecco un esempio di private key:

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

Ecco un esempio di public key (generata automaticamente con il suffisso .pub):

```
# cat /tmp/demo_key.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABA < --- SNIP --- > 6mEO5Gh28Vw== Commento per
chiave demo
```

4.3 Inviare la public key a PostFinance

Una copia della public key deve essere inviata per e-mail a PostFinance.

Servizio	Indirizzo e-mail
Traffico dei pagamenti	tscorp@postfinance.ch
Reconciliation Files / RAF	aqs@postfinance.ch
Altro	mftpf@postfinance.ch

Affinché PostFinance possa verificare la chiave ricevuta con il mittente, la persona di contatto deve inviare la chiave (in alternativa si deve procedere con uno scambio di e-mail). Una volta ricevuta la public key, una collaboratrice o un collaboratore di PostFinance si mette in contatto con la persona indicata per confrontare le ultime cifre del valore hash della public key generato con SHA256. In questo modo si può escludere qualsiasi manipolazione da parte di terzi.

Dopo aver installato la chiave, vi comunichiamo la conclusione dell'operazione. A quel punto potete testare il collegamento.

Gestite le private key come se si trattasse della vostra carta di credito.
Si prega di proteggerle da accessi non autorizzati.

4.4 Test del collegamento

Per testare il collegamento selezionate il nome host desiderato per la produzione o l'ambiente di test (cfr. capitolo 3.2 *Nome host, porta e indirizzi IP*).

Il nome utente, i dettagli sui nomi delle directory e i nomi dei file vengono comunicati nell'ambito dell'ordinazione del servizio.

4.4.1 Test del collegamento con Telnet

Il collegamento a MFTPF può essere verificato, ad esempio, con Telnet:

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

Attenzione: vengono utilizzati due indirizzi IP. Entrambi gli indirizzi IP possono essere determinati con risoluzione DNS (nslookup mftp1.postfinance.ch o nslookup mftt1.postfinance.ch) effettuando più tentativi. Essi possono essere utilizzati solo per configurare le regole del firewall. Per allestire il collegamento è obbligatorio utilizzare il nome DNS.

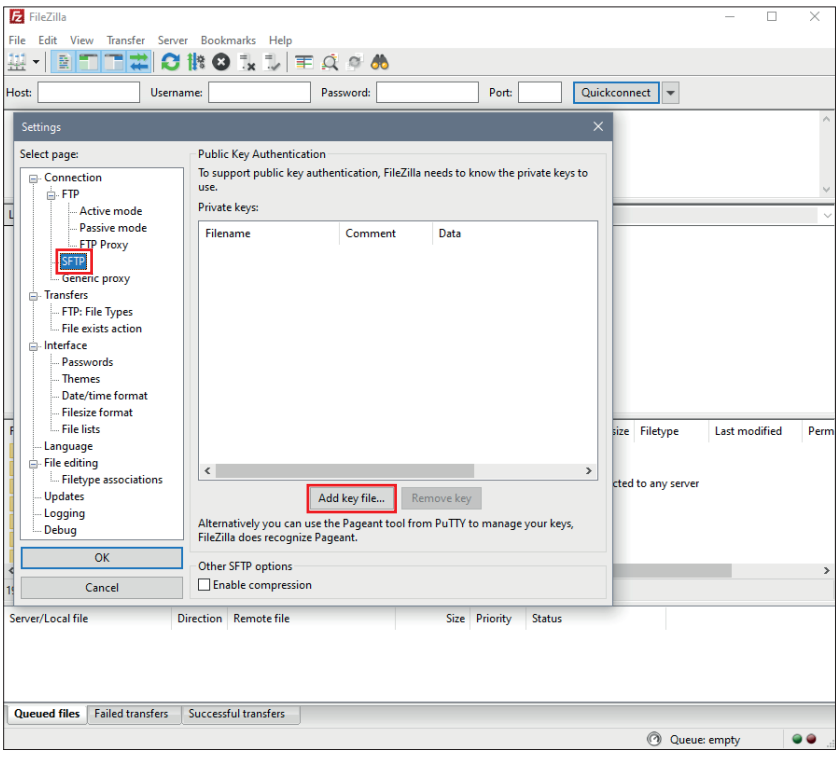
4.5 Configurazione FileZilla

4.5.1 Importazione della chiave con FileZilla

Per l'importazione la chiave può essere registrata con PuTTY o OpenSSH.

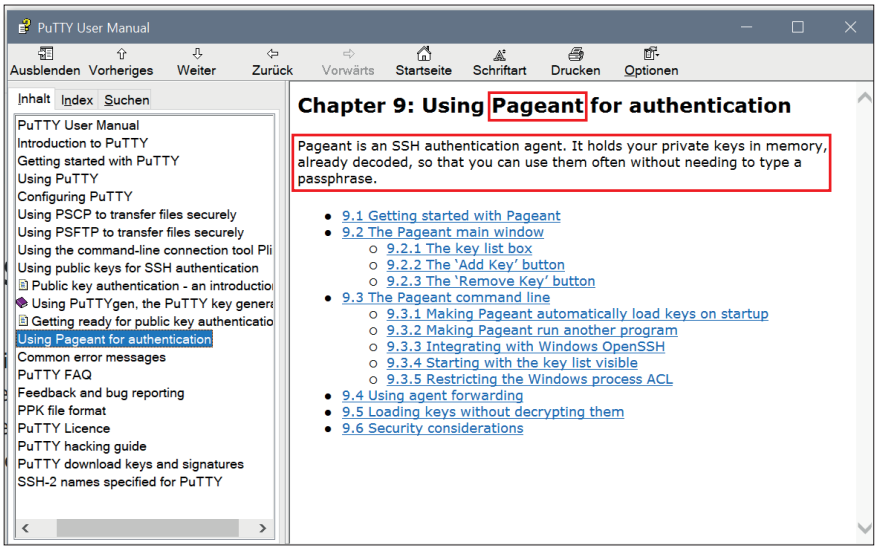
Avviare FileZilla.
Cliccare su *Modifica* e poi su *Impostazioni*.
Seleziona pagina: *SFTP*
Cliccare su *Aggiungi file chiave.*

Inserire la private key generata in precedenza.

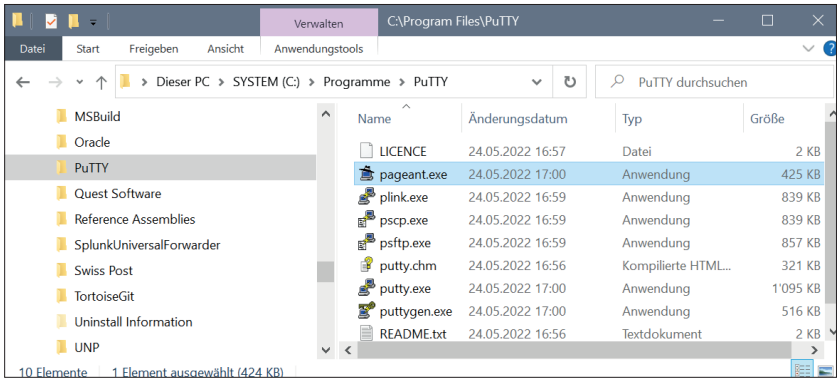


4.5.2 Importazione automatica con il Pageant di PuTTY

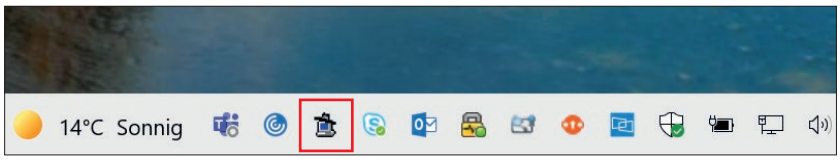
Attenzione: per poter utilizzare il Pageant di PuTTY la chiave deve essere generata con PuTTY.
Il *Pageant* (PuTTY Authentication Agent) è un agent SSH con il quale è possibile trasmettere le autenticazioni SSH. Il Pageant può caricare le chiavi e rendere disponibili, su richiesta, questi programmi locali. L'interfaccia è aperta, cosicché altri programmi possono collegarsi a questo servizio di Pageant.



Avviare pageant.exe.

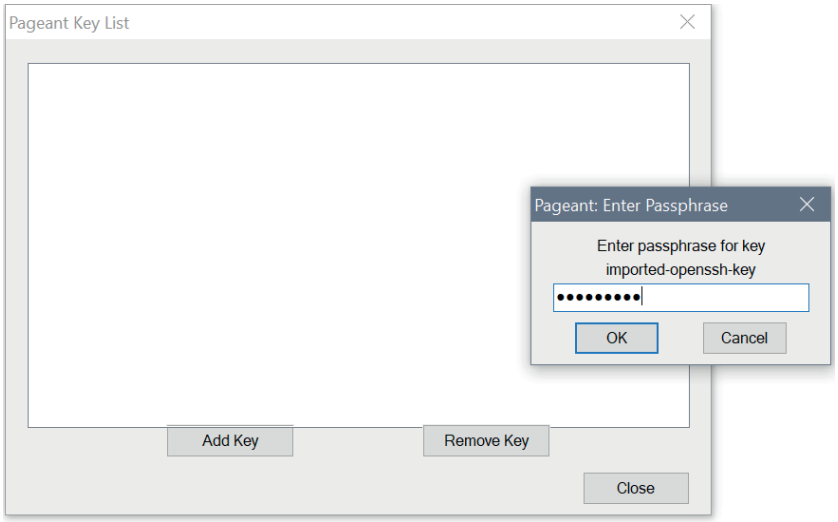


Pageant si trova nella system tray a destra in basso, nella barra di avvio veloce e contiene tutte le sessioni salvate in Pageant.



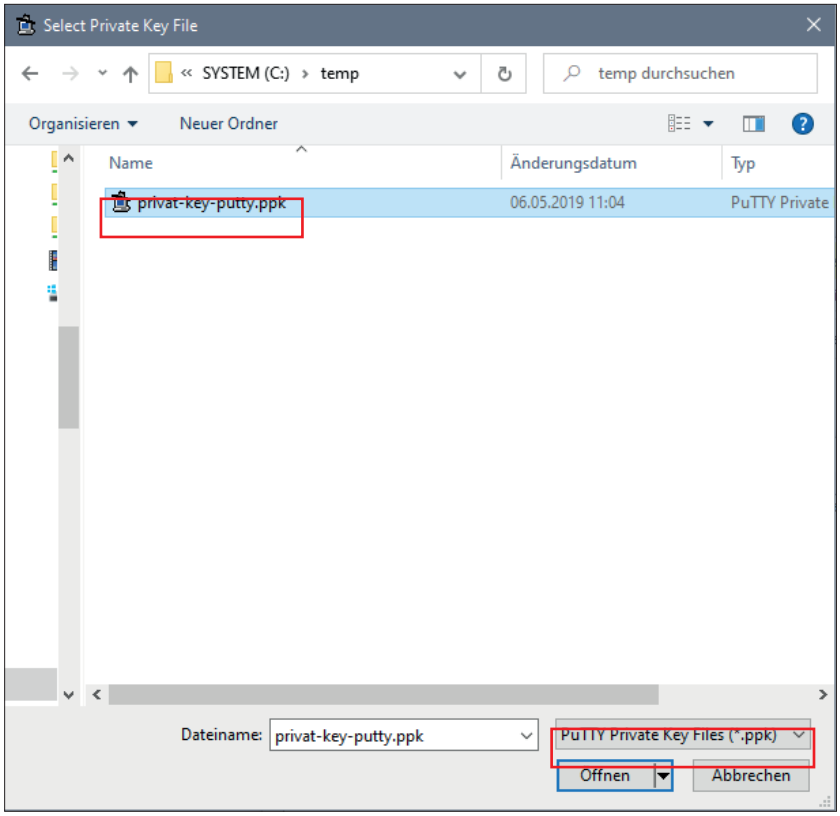
Fare doppio clic sull'icona del cappello.

Cliccare su *Add Key* per aprire la finestra in cui verrà selezionata la private key.

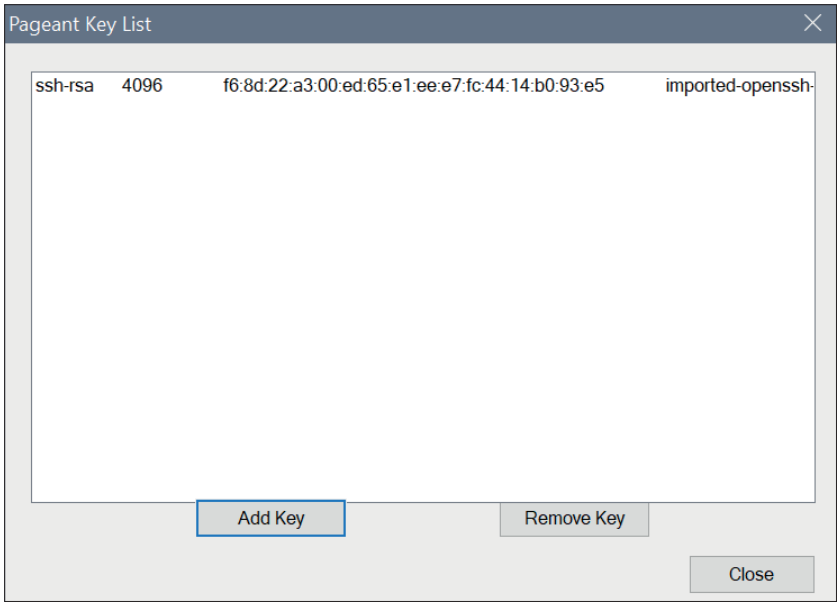


Selezionare la private key e confermare con *Apri*.

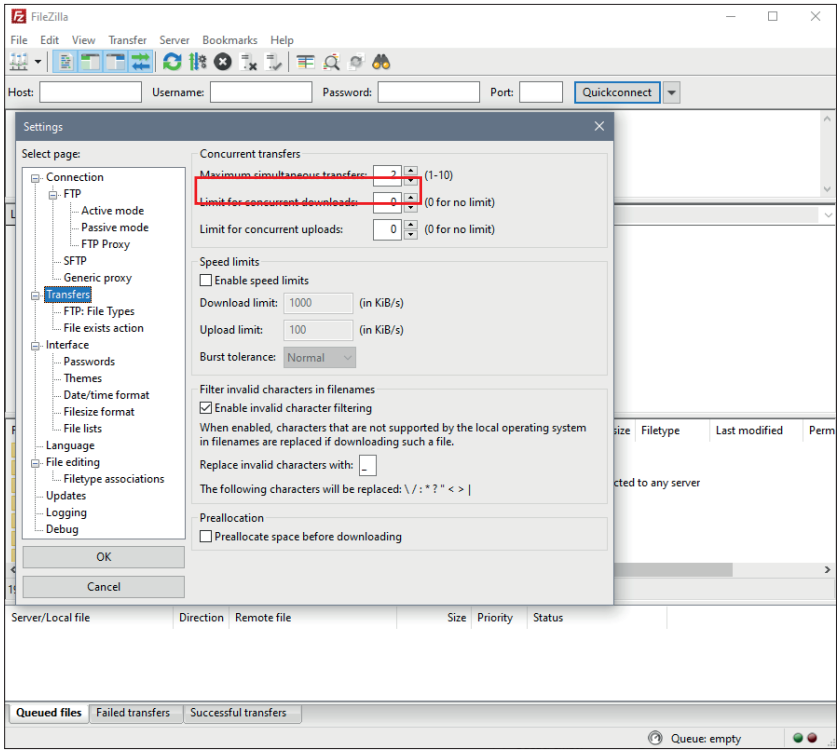
Attenzione: possono essere importate solo chiavi generate con PuTTY.



La chiave importata correttamente dovrebbe apparire come nell'esempio qui accanto.



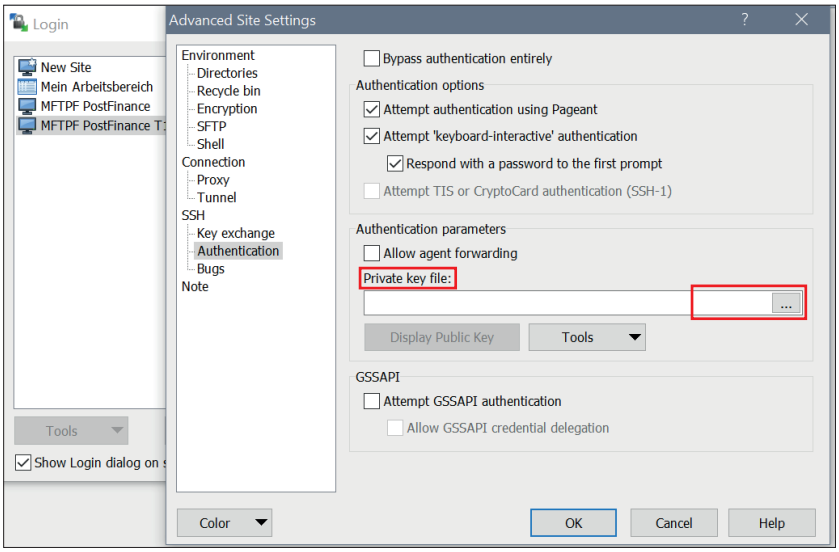
Nota:
Per non essere bloccati, consigliamo di limitare a *tre* il numero massimo di trasferimenti contemporanei.



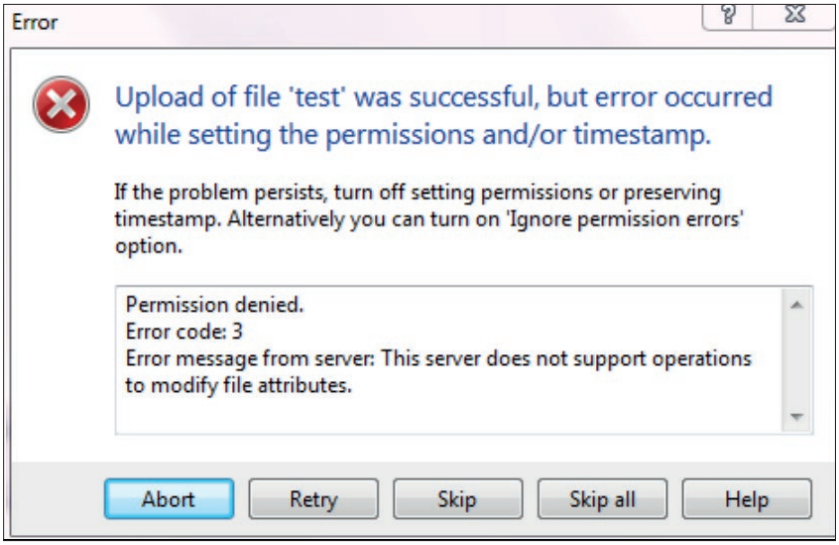
4.6 Configurazione WinSCP

4.6.1 Importazione della chiave con WinSCP

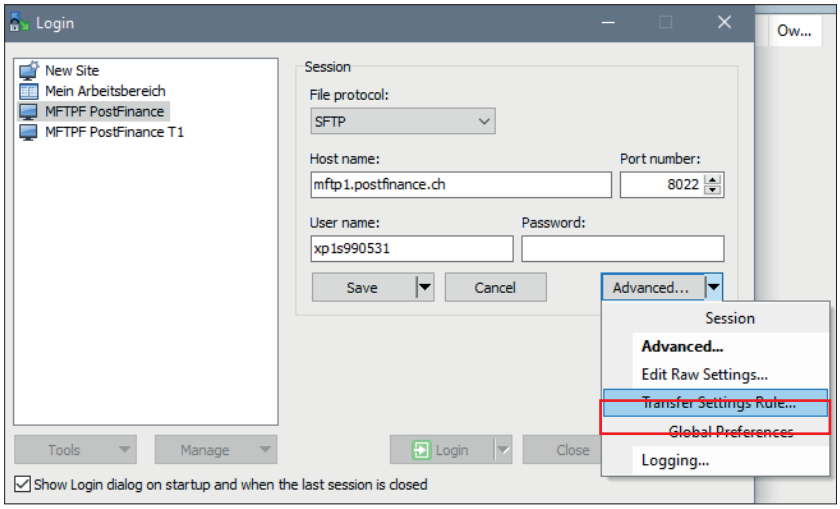
Avviare WinSCP.
Avanzate
Autenticazione
Cliccare su *File chiave privata* [...]
e selezionare la private key.



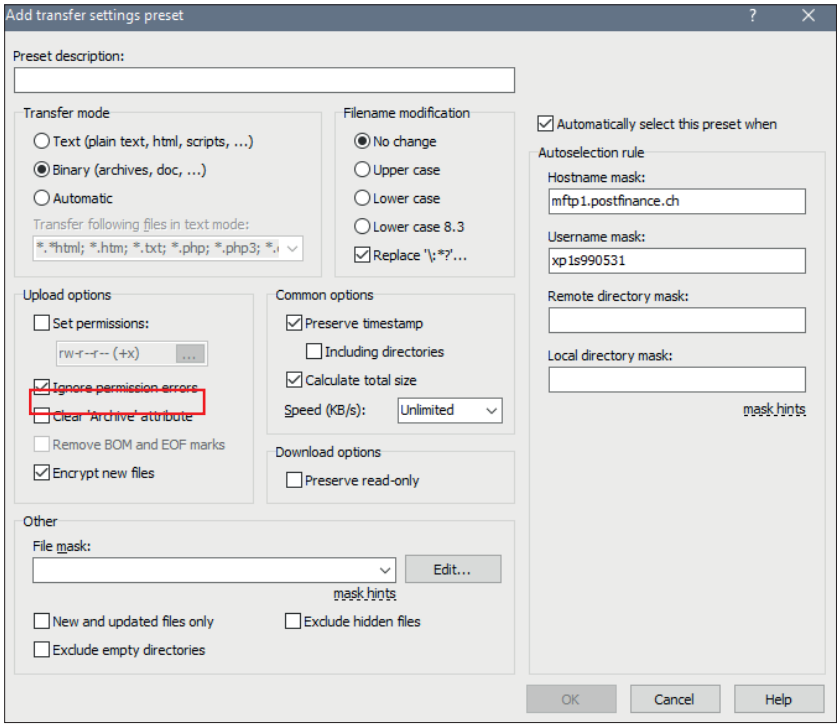
I problemi di autorizzazione dopo il caricamento come quelli riportati nella schermata qui accanto possono essere risolti modificando le impostazioni.



Andare su
Avanzate
Regola Impostazioni Trasferimento
e scegliete questa opzione.



Spuntate la casella
Ignora errori sui permessi.



5. Informazioni sull'impiego di MFTPF

La presente nota informativa descrive lo scambio di dati e le funzioni di MFTPF e presenta le regole e i requisiti generalmente validi per la trasmissione di file tramite i server di MFTPF.

5.1 Condizioni quadro/limitazioni

a) MFTPF non è un sistema di archiviazione. I file da scaricare non ancora cancellati dal/dalla cliente vengono in ogni caso eliminati automaticamente dal server dopo nove giorni.
b) Per trasmettere molti file è necessario ricorrere a un numero corrispondente di trasferimenti di file (put/get) per sessione di login SFTP. Ad esempio per 1200 file: 10 collegamenti/login ognuno con esecuzione di 120 trasferimenti di file. Se il numero di login durante determinate unità temporali è troppo elevato, l'Intrusion Prevention System di PostFinance blocca automaticamente per 15 minuti i Source IP-Address incriminati.
c) MFTPF non conferma al mittente il trasferimento dei file, dunque non invia alcuna notifica al momento della ricezione. La creazione e l'invio di ricevute di conferma (ad es. per le notifiche pain.001 in entrata vengono preparate notifiche pain.002) spettano ai sistemi di ricezione e non sono garantiti da MFTPF.
d) Al trasferimento dei file, in caso di inoltro non è garantita alcuna sequenza di trasmissione. I file di dimensioni differenti possono sovrapporsi in una sequenza parallela. Il sistema di ricezione della relazione end-to-end è responsabile per la riproduzione della corretta sequenza dei file trasmessi.
e) L'inoltro e la distribuzione dei file sono controllati per evento. Non è possibile utilizzare un controllo temporale.

Limitazione della trasmissione dei dati (client → server MFTPF)
- In caso di upload (put) da parte di un client di trasferimento file in una directory MFTPF, i file vengono direttamente elaborati dai processi sul server MFTPF alla conclusione del trasferimento. Le registrazioni dei file nelle mailbox di upload rimangono tuttavia visualizzabili dal/dalla cliente per due minuti (visualizzazione dei file tramite «dir» e «ls»). La cancellazione o la rinomina di un file trasmesso non ha senso: il file viene inoltrato al/la destinatario/a con il nome di file originario.
- MFTPF assicura che vengano elaborati solo file trasmessi integralmente. In caso di interruzione del collegamento, il file incompleto viene respinto.
- Con MFTPF non è possibile modificare gli attributi del file dopo il loro trasferimento.