Manuale d’esercizio «File Transfer Client»

File Delivery Services

Editore

Posta CH SA
Informatica
Webergutstrasse 12
CH-3030 Berna (Zollikofen)

Contatto

Posta CH SA
Informatica
Webergutstrasse 12
CH-3030 Berna (Zollikofen)
IT17.34 FDS
E-mail: fds@posta.ch

Versione 5.2 / gennaio 2023

La versione attuale è disponibile su: https://www.posta.ch/fds

Indice

1. Aspetti generali

1.1 Scopo

Gli utenti FDS possono impiegare un client per il trasferimento file scelto a piacere.

In questo documento e descritto la creazione e la configurazione delle SSH Keys ed in complemento ci sono delle indicazioni importanti per l'utilizzo dei due Software più diffusi (WinSCP e FileZilla).

Anche se le precedenti e future versioni di software, nonché altri client sftp dovrebbero, in linea di massima, funzionare senza problemi con l'FDS, in caso di problemi nonché per l'implementazione di soluzioni di trasferimento file, Posta Informatica può offrire solo un supporto limitato.

1.2 Definizioni, acronimi e abbreviazioni

Parola	Definizione
ssh	Il termine SSH o Secure Shell 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.
scp	Secure Copy o SCP è un protocollo per la trasmissione cifrata di dati tra due computer mediante una rete informatica.
sftp	SFTP o SSH File Transfer Protocol è una fase successiva dell'SCP e consente il trasferimento sicuro dei dati a sistemi remoti.
PuTTY	PuTTY è un client SSH gratuito, sviluppato da Simon Tatham per Microsoft Windows.

2. SFTP

2.1 Introduzione

L'SFTP (SSH Secure File Transfer Protocol) è un protocollo di trasferimento dati sicuro. Tra client e server viene infatti stabilito un collegamento ininterrotto e cifrato tramite il quale i dati e i nomi utente risultano illeggibili per eventuali intrusi. L'SSH garantisce la trasmissione completa e integrale dei dati dal mittente al destinatario.

Attenzione: l'SFTP non va confuso con l'FTPS (FTP mediante SSL) o con l'FTP mediante SSH (detto talvolta Secure FTP).

L'FDS SFTP Server supporta:

- versione 2 di SSH
- versione 3 del protocollo SFTP
- comandi SCP in ingresso mediante protocollo SSH/SCP Importante: SCP non supporta list, rename e delete
- trasmissioni di file fino a un volume massimo di 50 GB
- 200 collegamenti contemporanei dallo stesso account
- blocco dell'account per 30 minuti dopo 5 tentativi di login errati
- le chiavi supportate sono quelle in formato openSSH, ssh.com e PuTTY
- per ciascun account possono essere configurate 1 o più chiavi

L'FDS SFTP Server non supporta:

- versione 1 di SSH
- sedute Shell interattive
- ripresa di trasmissioni
- modifiche di attributi del file
- manipolazione della struttura della directory

2.2 Sicurezza

I clienti FDS devono garantire che il loro software di trasferimento di file siano aggiornati. È particolarmente importante che vengono utilizzati algoritmi di cifratura considerati sicuri e codici di autenticazione dei messaggi (MAC).

La Posta CH SA e le sue unità di servizio e d'affari non assumono nessuna responsabilità e non è responsabile per danni causati da uso di algoritmi non sicuri e / o metodi di MAC.

2.2.1 Algoritmi di crittografia

L'algoritmo AES deve essere selezionato. La lunghezza minima della chiave deve essere 128 bit.

La Tecnologia dell'Informazione della Posta si riserva il diritto di non sostenere più senza preavviso algoritmi vecchi e algoritmi con una lunghezza della chiave <128 bit.

2.2.2 Message Authentication Codes (MAC)

MAC è un critto sistema basato su chiavi simmetriche con lo scopo di garantire l'integrità dei messaggi.

Il metodo MAC consentito è hmac-sha2-256 o hmac-sha2-512

La Tecnologia dell'Informazione della Posta si riserva il diritto di non sostenere più senza preavviso metodi MAC obsoleti, come hmac-sha1.

2.3 Public e Private Key

Il metodo più semplice di autentificazione è la password. Anche se è criptata, esistono dei programmi capaci di rompere la criptazione.
Per questo motivo, l'unico metodo di autentificazione accettato sul nostro server FDS è l'uso di coppie di chiavi SSH.

Le coppie di chiavi SSH sono chiavi asimmetriche, il che significa che le due chiavi associate hanno funzioni diverse.
La chiave pubblica viene utilizzata per crittografare i dati che possono essere decifrati solo con la chiave privata.
La chiave pubblica può essere condivisa liberamente, perché sebbene possa criptare i dati per la chiave privata, non esiste un metodo in grado di dedurre la chiave privata dalla chiave pubblica.

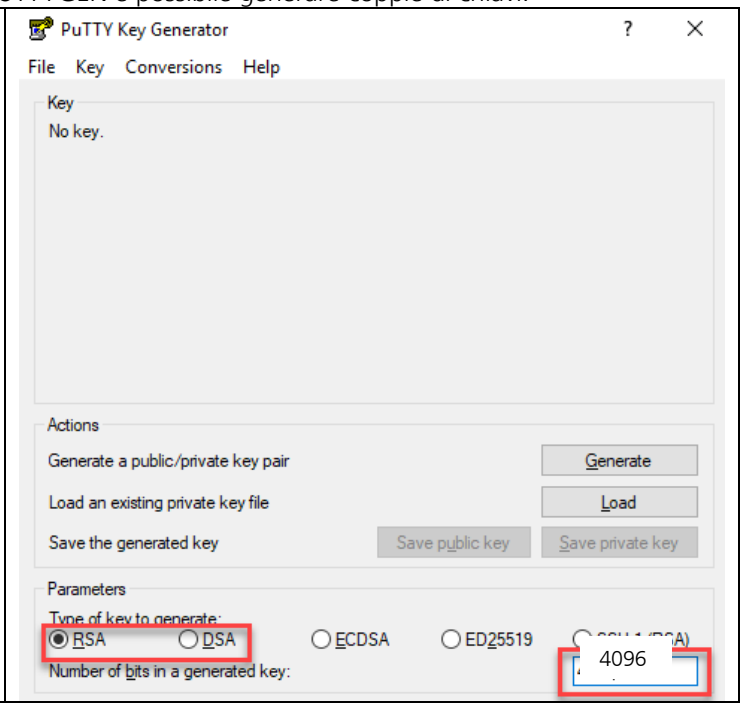
- La PUBLIC Key deve essere consegnata alla Posta (come da istruzioni della lettera di conferma FDS) e viene salvata sul server FDS della Posta
- La Private Key deve rimanere sempre nel vostro PC e non va MAI trasmessa a terzi
- La coppia di chiavi deve essere generata dal cliente FDS
- FDS supporta il sistema di crittografia «RSA» (Rivest-Shamir-Adleman)
- Le chiavi generate devono avere una lunghezza di minimo **4096** bit.

NOTA: Affinché la Private Key sia protetta dall'uso non autorizzato, si consiglia di generarla con una passphrase. Si deve però considerare che, a seconda del software utilizzato, in tal modo l'automazione del login può risultare più difficile.

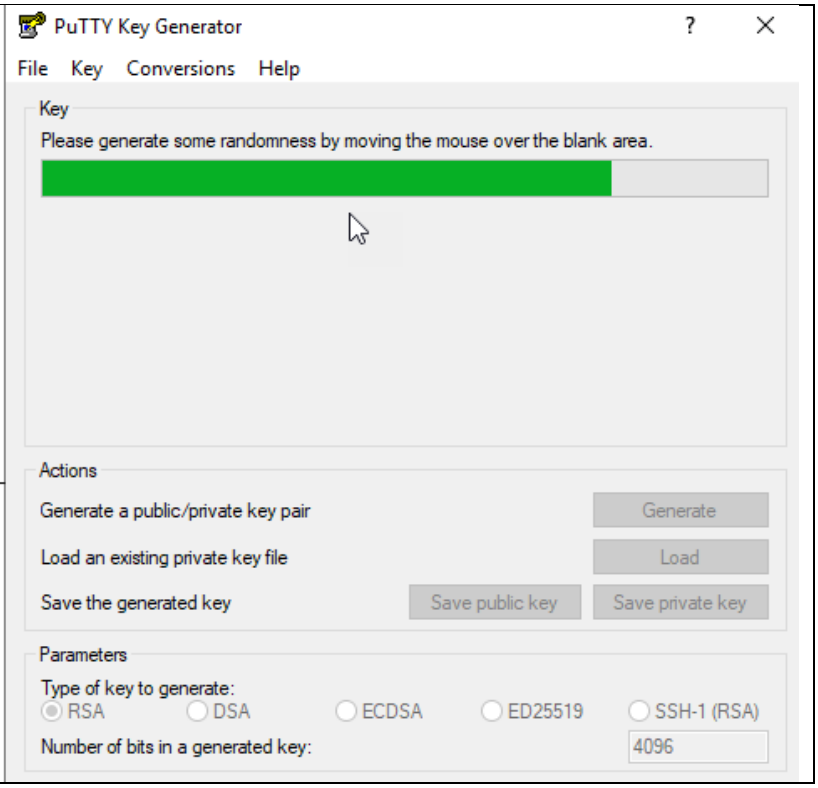
2.3.1 Creazione di una coppia di chiavi SSH con PuTTY

PuTTY è un software Open Source per Microsoft Windows. Può essere scaricato da http://www.putty.org.

Accanto a un SSH/SFTP-Client (putty.exe), con PUTTYGEN è possibile generare coppie di chiavi.

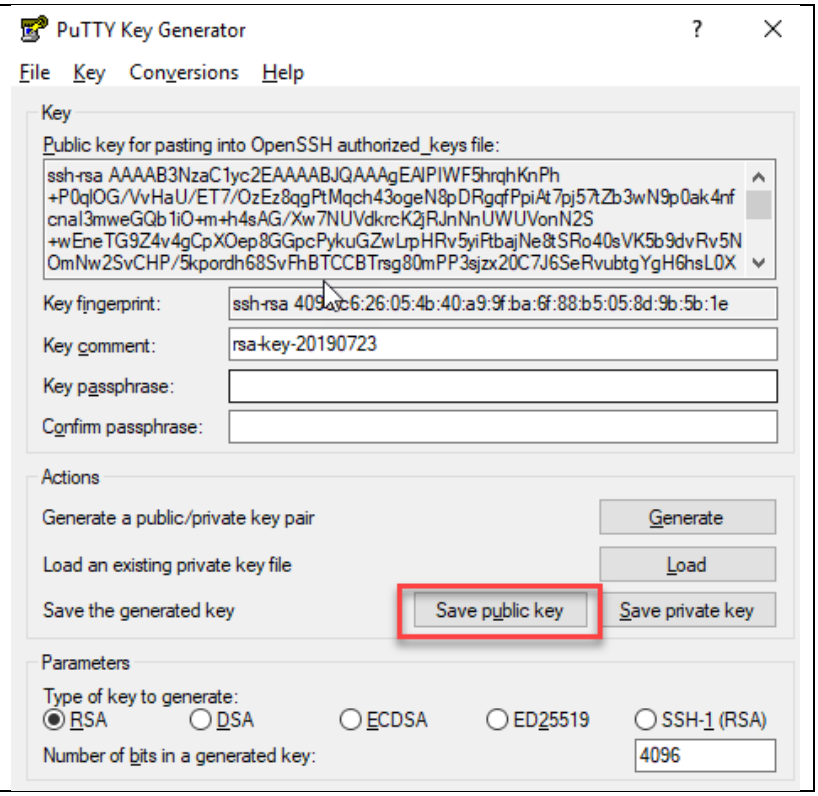
Avviare PUTTYGEN Verificare se sono stati selezionati RSA e almeno 4096 (bit), quindi fare clic su «Generate»	

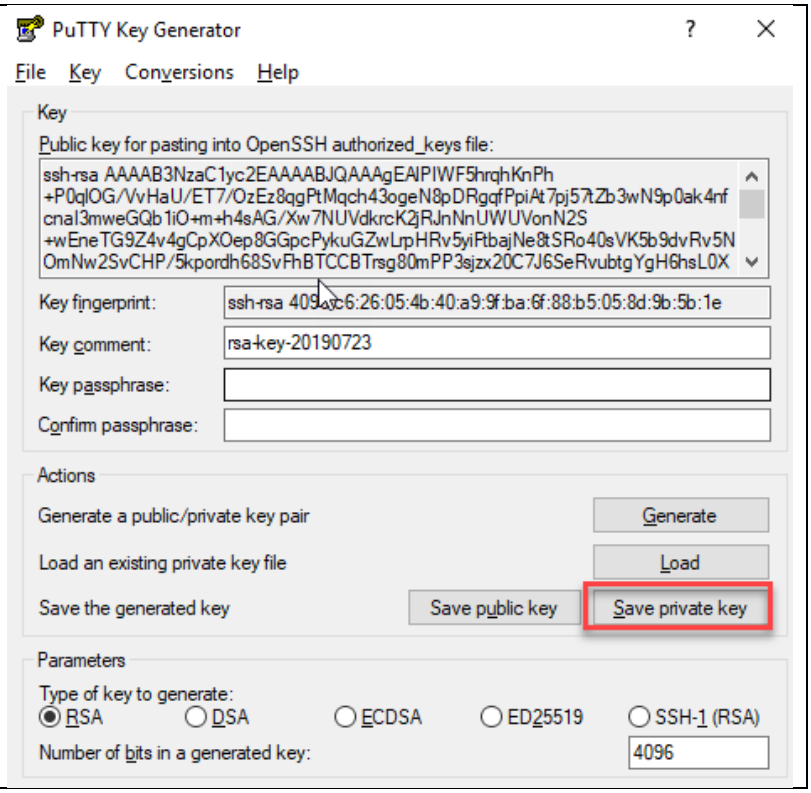
Muovere il cursore del mouse sulla superficie sotto la barra blu



Al termine dell'operazione compare la maschera con le chiavi

Selezionare «Save public key»



Selezionare «Save private key» ATTENZIONE: la Private Key deve rimanere sempre nel vostro PC e non va MAI trasmessa a terzi Affinché la Private Key sia protetta dall'uso non autorizzato, si consiglia di generarla con una passphrase. Si deve però considerare che, a seconda del software utilizzato, in tal modo l'automazione del login può risultare più difficile. In questo esempio si prosegue senza passphrase	

2.3.2 Creazione di una coppia di chiavi SSH con OpenSSH

OpenSSH è disponibile come pacchetto di programma su tutte le piattaforme Unix.
Ulteriori informazioni su OpenSSH sono disponibili su http://www.openssh.com.

La coppia di chiavi può essere generata ad esempio 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 (viene generata automaticamente con il suffisso .pub):

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

3. Collegamento a FDS

3.1 Introduzione

È possibile accedere al server FDS tramite gli indirizzi fdsbc.post.ch (internet, linee noleggiate/IPSS) o fdsbc.pnet.ch (rete postale/DMZ della Posta).

I protocolli FDS utilizzano le porte standard (21 per FTP e 22 per SFTP).

Il nome utente e dettagli relativi a nomi delle directory e dei file, tempi di trasmissione ecc. vengono comunicati nell'ambito dell'ordinazione del servizio.

Le finestre di manutenzione previste vengono pubblicate su https://www.posta.ch/fds.

3.2 Test del collegamento

Il collegamento a FDS può essere testato tramite *telnet*:

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

Attenzione: vengono utilizzati due indirizzi IP. I due indirizzi IP possono essere determinati per mezzo di risoluzione DNS traverso diversi tentativi (nslookup fdsbc.post.ch).
Gli indirizzi IP possono essere utilizzati solo per la configurazione delle regole del firewall. Per stabilire la connessione è bisogna assolutamente usare il nome DNS.

Se il server FDS non può essere raggiunto, deve essere controllato che la connessione non venga bloccata dal vostro firewall.

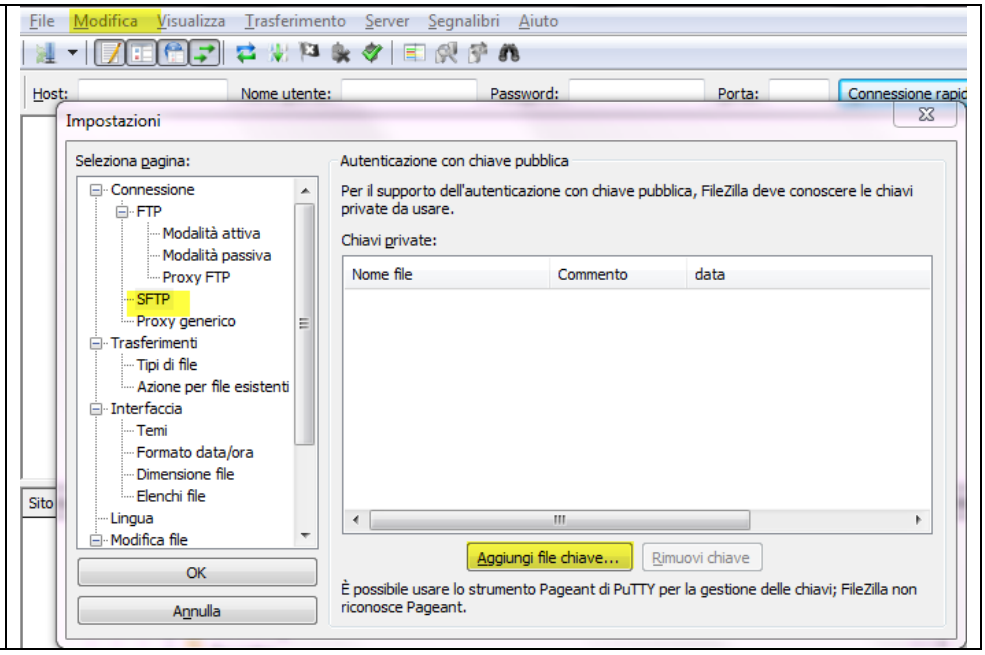
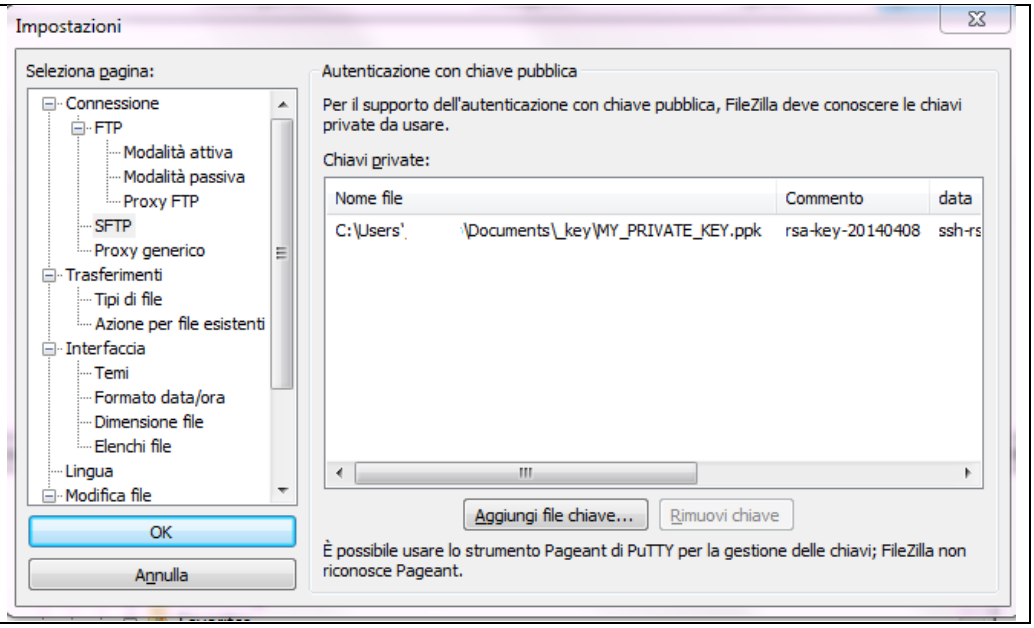
Se non fosse possibile collegarsi al server FDS, è necessario controllare se il proprio firewall blocca il collegamento.

Affinché Tecnologia dell'informazione della Posta possa fornire aiuto in modo efficace, è importante fornire le necessarie informazioni (nome di utente, messaggio d'errore, ora esatta del tentativo, nome del file e della directory)

4. FileZilla

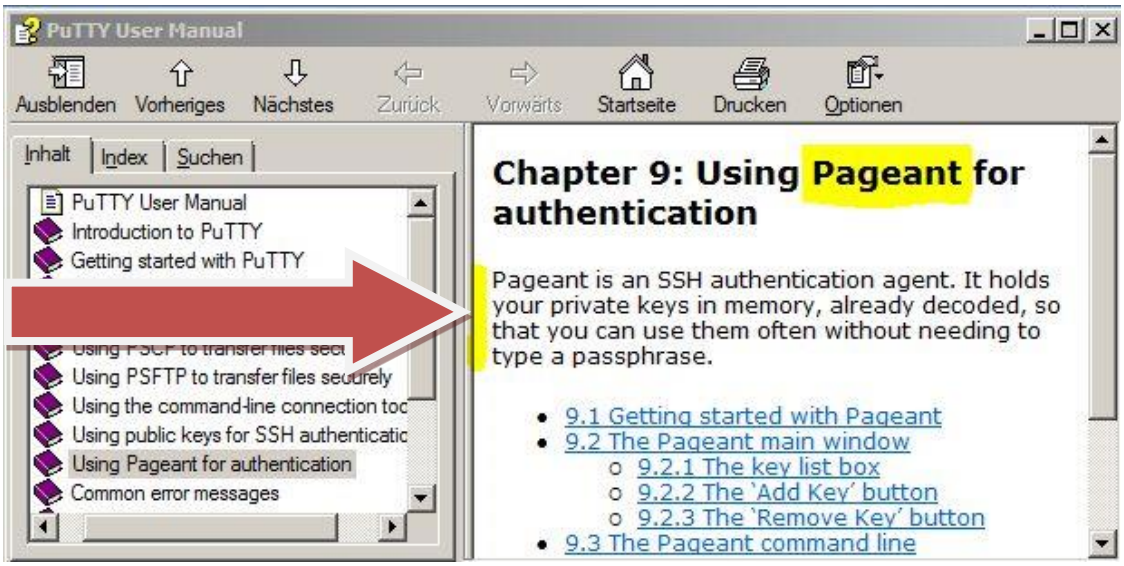
4.1 Importazione della chiave con FileZilla

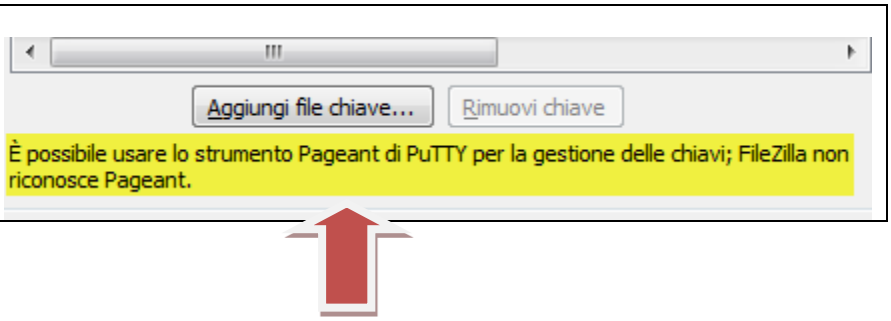
È possibile importare in FileZilla chiavi sia in formato PUTTY, sia in formato OpenSSH.

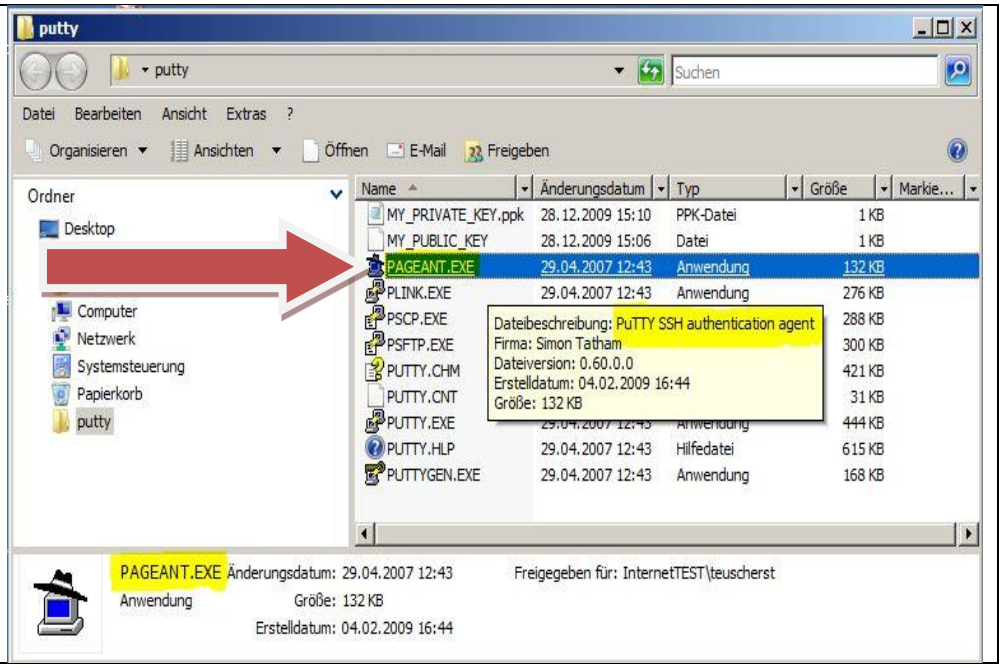
Avviare FileZilla 1) Menu **Modifica** 2) Menu **Impostazioni** (si apre una finestra) => SFTP => Aggiungi file chiave (quindi selezionare il file della private key giusto)	
Questa riga (gialla) indica che la chiave è stata importata correttamente.	

~~4.3~~4.2 Importazione automatica con il Pageant di 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, programmi locali. L'interfaccia è aperta, cosicché altri programmi possono collegarsi a questo servizio di Pageant.

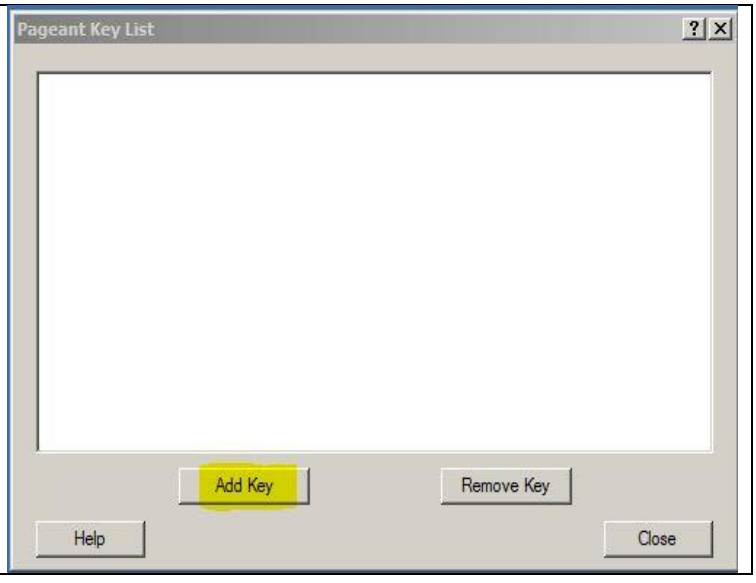


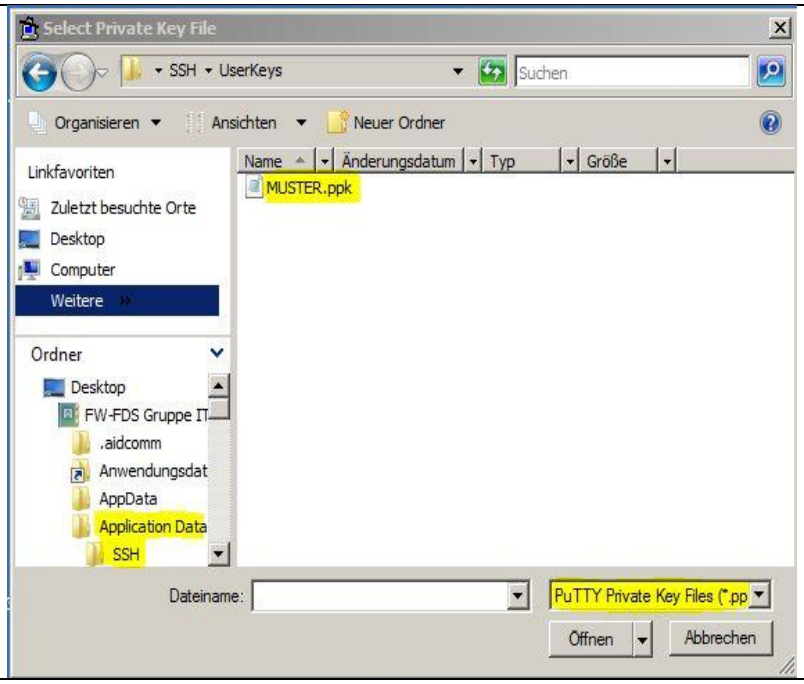
Avvertenza sul Pageant di PuTTY in FileZilla	

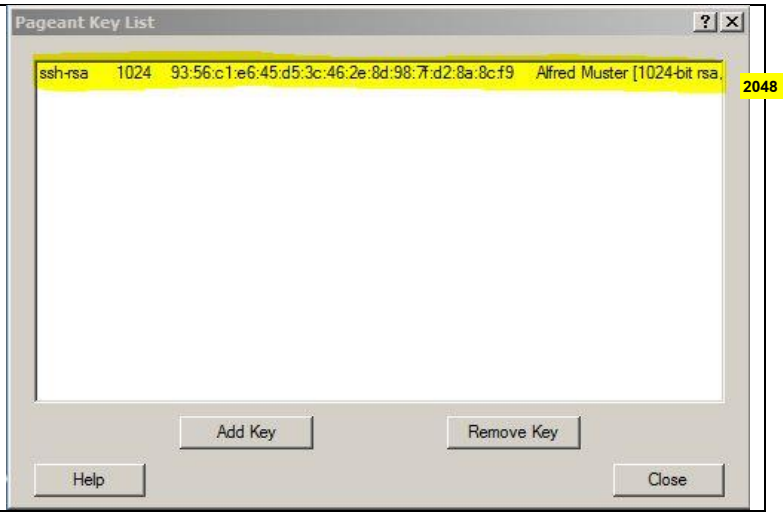
Avviare PAGEANT.EXE	

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

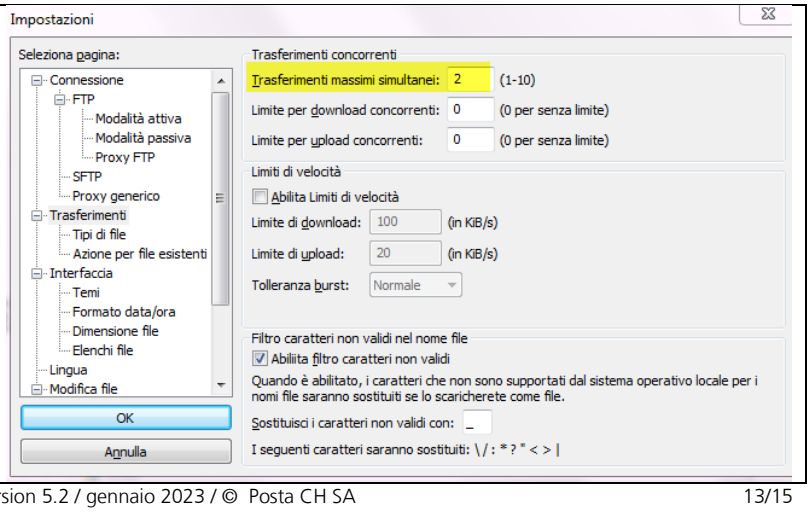
Quest'icona compare nella barra delle applicazioni:	

Doppio clic "sul cappello" nella system tray: Dopo l'apertura compare la finestra «Pageant Key List» (ancora) vuota:	

Mediante «Add Key», selezionare la private key e confermare con «Apri». Qui viene accettato solamente il formato PuTTY.	

Se la chiave viene visualizzata come nell'esempio seguente, è stata caricata correttamente e si trova nella memoria del PC. Diversi programmi SSH e soprattutto FileZilla hanno accesso diretto alla chiave dalla memoria.	

4.44.3 Note su FileZilla

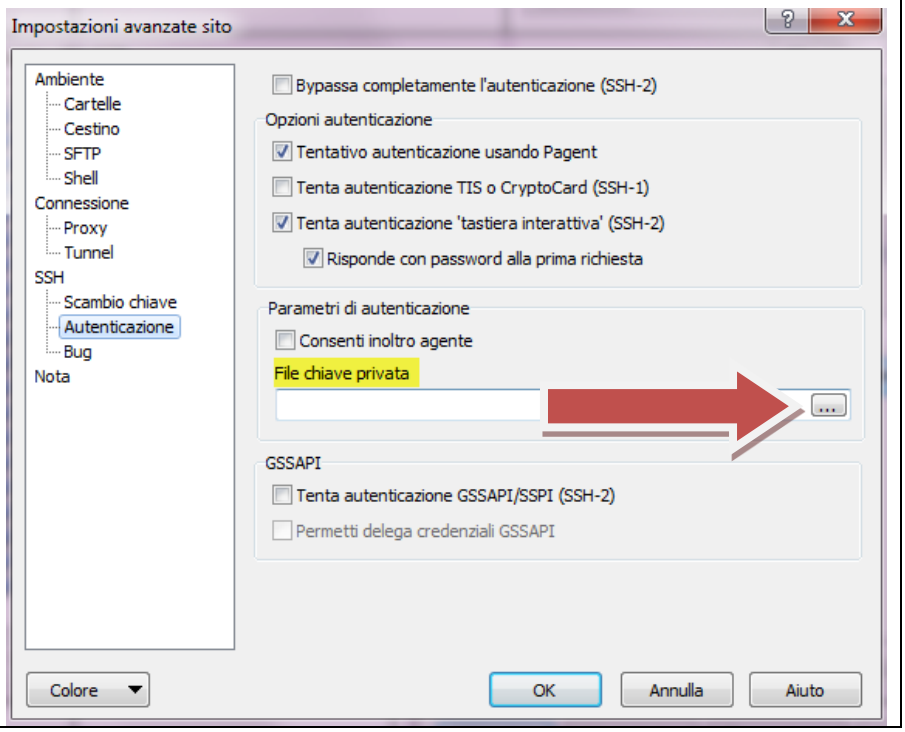
La Posta CH SA utilizza, tra i suoi meccanismi di protezione, anche un sistema IDS/IPS. Per non essere bloccati, consigliamo di limitare a uno o tre al massimo il numero di trasferimenti contemporanei	

5. WinSCP

5.1 Importazione della chiave con WinSCP

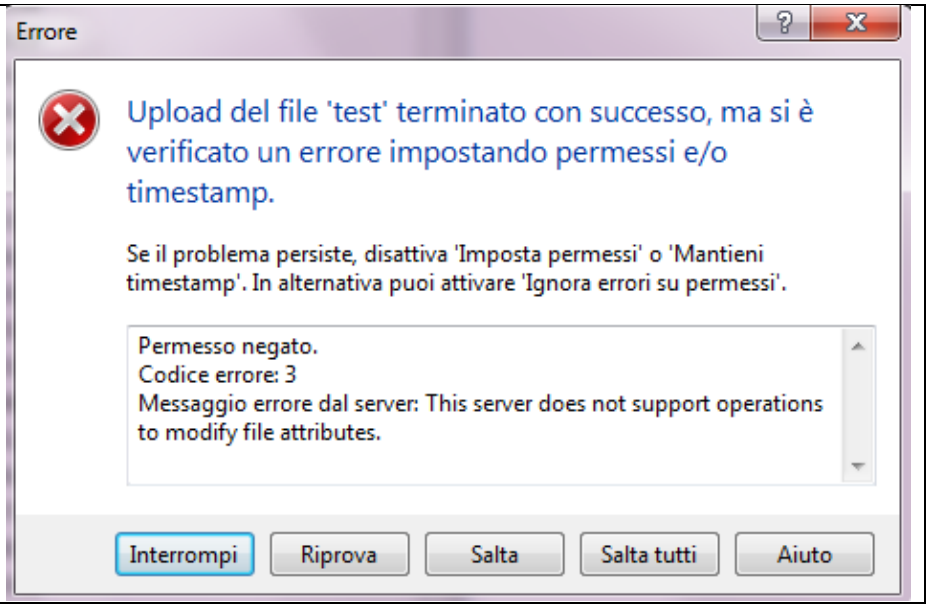
1) Avviare WinSCP
2) Fare clic su "Modifica"
3) Fare clic su"Avanziate …"

Fare clic sul campo «Apri» ➔ […]
e selezionare la private key.

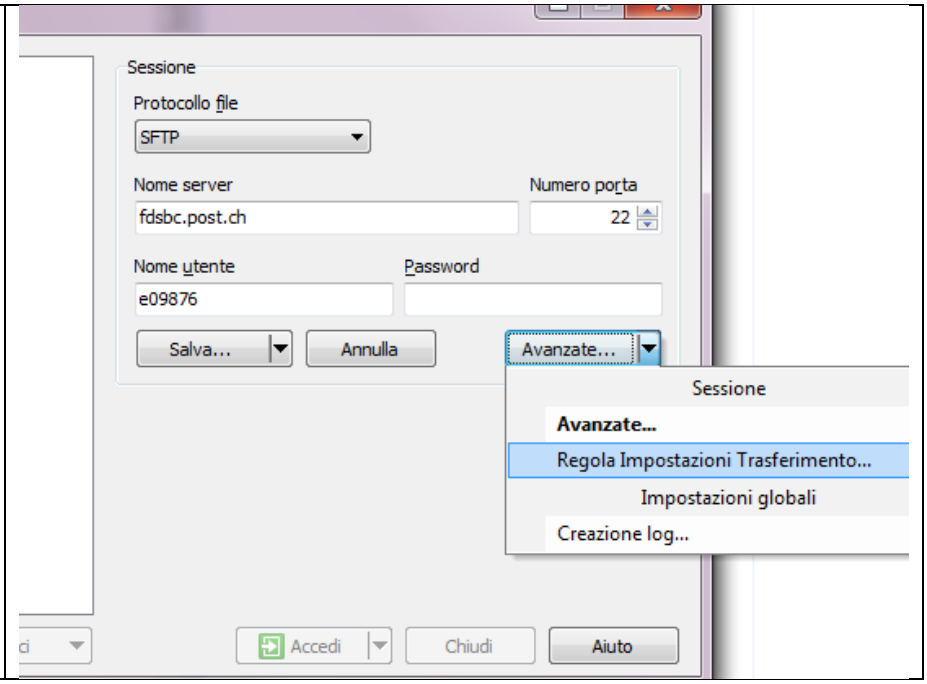


5.2 Nota sul WinSCP

Se si verificano problemi con le autorizzazioni dopo la trasmissione dei file…



… potete rimuoverli andando in «Avanzate …» → "Regola Impostazioni Trasferimento" …



=> disattivare l'opzione «Imposta permessi» e attivare i campi «Ignora errori sui permessi».