Filetransfer-Clients Handbuch

File Delivery Services

Herausgeber

Post CH AG
Informatik
Webergutstrasse 12
CH-3030 Bern (Zollikofen)

Kontakt

Post CH AG
Informatik
Webergutstrasse 12
CH-3030 Bern (Zollikofen)
IT17.34 FDS Betrieb
E-Mail: fds@post.ch

Version 5.2 / Januar 2023

Download der aktuellen Version: https://www.post.ch/fds

Inhaltsverzeichnis

1. Allgemeines

1.1 Einleitung

Die FDS-Benutzer dürfen den Filetransfer-Client ihrer Wahl einsetzen.

In diesem Dokument werden die Erstellung und Konfiguration von SSH Keys sowie wichtige Hinweise zu 2 meist benutzen Software (WinSCP und FileZilla) beschrieben. Obwohl vorherige und zukünftige Software Versionen wie auch andere sftp-Clients grundsätzlich mit FDS einwandfrei funktionieren sollten, kann Informatik Post bei Problemen sowie bei der Implementierung von Filetransfer-Lösungen nur beschränkt Unterstützung bieten.

1.2 Definitionen, Akronyme und Abkürzungen

Wort	Definition
ssh	SSH oder Secure Shell bezeichnet sowohl ein Netzwerkprotokoll als auch entsprechende Programme, mit deren Hilfe man auf eine sichere Art und Weise eine verschlüsselte Netzwerkverbindung mit einem entfernten Computer herstellen kann.
scp	Secure Copy oder SCP ist ein Protokoll zur verschlüsselten Übertragung von Daten zwischen zwei Computern über ein Rechnernetz.
sftp	SFTP oder SSH File Transfer Protocol ist eine Weiterentwicklung von SCP und erlaubt sichere Datenübertragung auf entfernte Systeme.
PuTTY	PuTTY ist ein von Simon Tatham entwickelter freier SSH-Client für Microsoft Windows.

2. SFTP

2.1 Einleitung

SFTP (SSH Secure File Transfer Protocol) ist ein sicheres Filetransferprotokoll. Zwischen Client und Server wird eine ununterbrochene, verschlüsselte Verbindung hergestellt, welche die Daten und Benutzernamen für einen Angreifer unlesbar machen. SSH garantiert das vollständige und unveränderte Übertragen der Daten vom Absender zum Empfänger.

Achtung: SFTP ist nicht mit FTPS (FTP über SSL) oder mit FTP über SSH (manchmal Secure FTP genannt) zu verwechseln.

Der FDS SFTP Server unterstützt:

- Version 2 SSH
- Version 3 SFTP Protokoll
- eingehende SCP Befehle mittels SSH/SCP Protokoll. Zur Beachtung: SCP unterstützt list, rename und delete nicht.
- Übertragungen von Dateien bis 50 Gigabytes Grösse.
- 200 gleichzeitige Verbindungen vom gleichen Account
- Account Sperrung für 30 Minuten nach 5 fehlerhaften Login Versuche
- Unterstützt sind Keys im openSSH, ssh.com und PuTTY-Format
- Pro Account können 1 oder mehrere Keys konfiguriert werden

Der FDS SFTP Server unterstützt nicht:

- Version 1 SSH
- interaktive Shell-Sitzungen
- Wiederaufnahme von Übermittlungen
- die Änderungen von Dateiattributen
- die Manipulation der Verzeichnisstruktur

2.2 Sicherheit

Die FDS Kunden müssen sicherstellen, dass ihre Filetransfer-Software auf dem neusten Stand ist. Es ist insbesondere wichtig, dass nur als sicher geltende Verschlüsselungs-Algorithmen sowie Message Authentication Codes (MAC) eingesetzt werden.

Die Schweizerische Post und deren Service- und Geschäftsbereiche übernehmen keine Verantwortung und keine Haftung für Schäden die durch Einsatz von unsicheren Algorithmen und/oder MAC Verfahren entstehen.

2.2.1 Verschlüsselungs-Algorithmen

Der AES Algorithmus muss gewählt werden und dies mit einer minimalen Schlüssellänge von 128 bits.

Informatik Post behält sich das Recht vor, überholte Algorithmen sowie Algorithmen mit einer Schlüssellänge < 128 bits ohne Voranmeldung nicht mehr zu unterstützen.

2.2.2 Message Authentication Codes (MAC)

MAC sind ein auf symmetrischen Schlüsseln basierendes Krypto System mit dem Ziel die Integrität von Nachrichten zu garantieren.

Die zulässigen MAC Verfahren sind hmac-sha2-256 oder hmac-sha2-512.

Informatik Post behält sich das Recht vor, überholte MAC Verfahren wie zum Beispiel hmac-sha1 ohne Voranmeldung nicht mehr zu unterstützen.

2.3 Public-, und Private Key

Die einfachste Authentifizierungsmethode ist die Verwendung eines Passworts. Aber auch wenn dieses verschlüsselt ist, können automatisierte Skripte Passwörter relativ leicht knacken.
Aus diesem Grund ist die einzige zulässige Methode zur Authentifizierung auf unserem FDS-Server die Verwendung von SSH-Schlüsselpaaren.

SSH-Schlüsselpaare sind asymmetrische Schlüssel, was bedeutet, dass die beiden zugehörigen Schlüssel unterschiedliche Funktionen erfüllen.
Der öffentliche Schlüssel wird zur Verschlüsselung von Daten verwendet, die nur mit dem privaten Schlüssel entschlüsselt werden können.
Der öffentliche Schlüssel kann frei weitergegeben werden, da er zwar für den privaten Schlüssel verschlüsseln kann, es aber keine Methode gibt, den privaten Schlüssel vom öffentlichen Schlüssel abzuleiten.

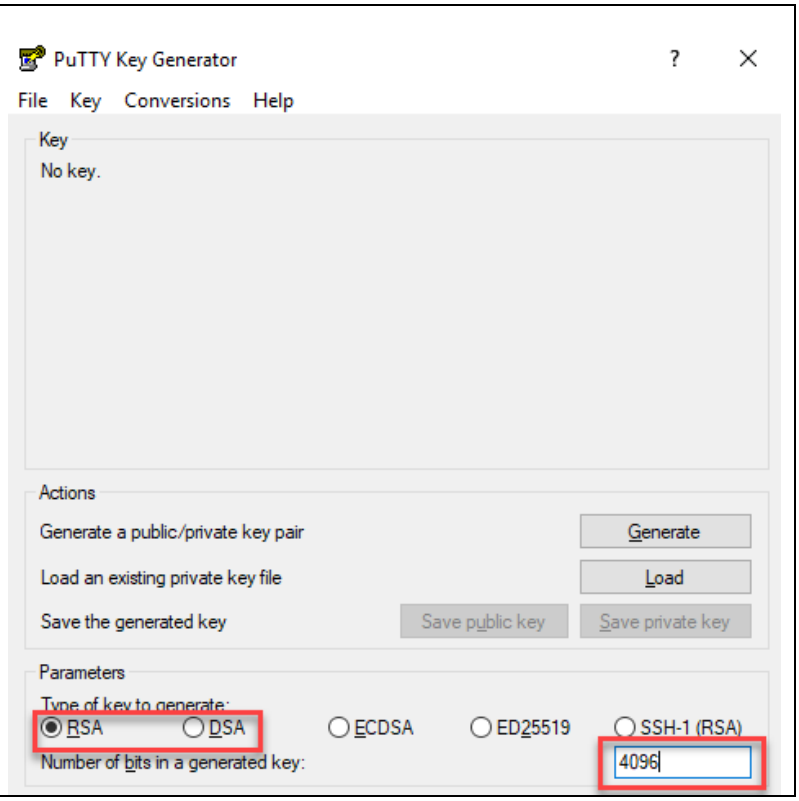
- Das Schlüssel-Paar muss durch den FDS-Kunden generiert werden.
- Der Public-Key muss uns gemäss Anleitung des FDS-Handbuchs zugestellt werden und wird auf dem FDS-Server der Post gespeichert.
- Der Private-Key darf NIE weitergegeben werden!
- FDS unterstützt das „RSA“ (Rivest-Shamir-Adleman) Krypto System. Bitte beachten: „DSA“ („Digital Signature Algorithm“) Krypto System ist nicht mehr unterstützt.
- Die Länge des generierten Keys muss mindestens **4096** bits sein.

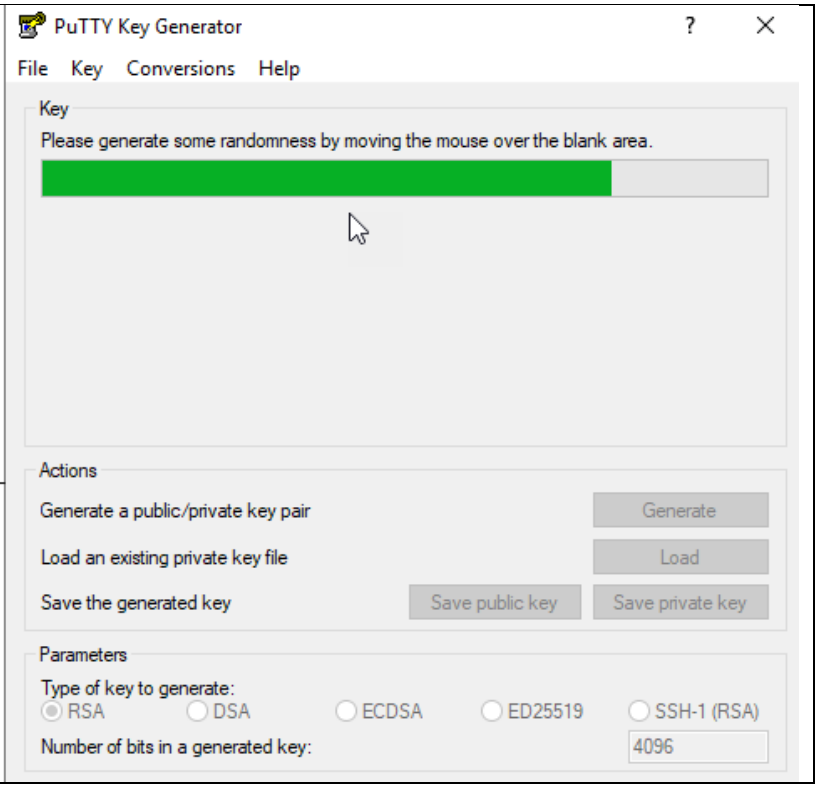
Hinweis: Damit der Private-Key vor unberechtigten Gebrauch geschützt wird, ist seine Generierung mit einer Passphrase empfohlen. Man muss aber beachten, dass je nach eingesetzter Software eine Automatisierung der Anmeldung dadurch erschwert werden kann.

2.3.1 Erstellen eines SSH-Schlüssel-Paares mit PuTTY

PuTTY ist eine Open Source Software für Microsoft Windows. Sie kann unter http://www.putty.org heruntergeladen werden

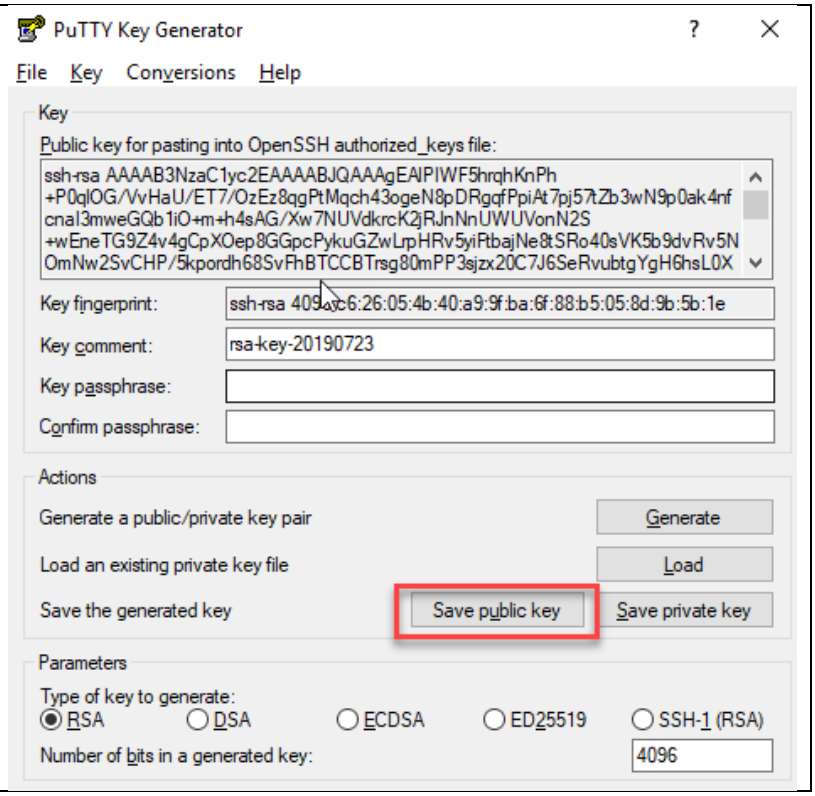
Neben einen SSH/SFTP-Client (putty.exe) gibt es mit PUTTYgen die Möglichkeit, Schlüssel-Paare zu generieren

PuTTYgen starten Kontrolle ob RSA als Schlüssel-Typ sowie mindestens 4096 bits angewählt sind, nachher: „Generate“ anklicken	

Maus-Cursor über die Fläche unter dem blauen Balken bewegen	

Wenn fertig, erscheint die Maske mit den Keys.

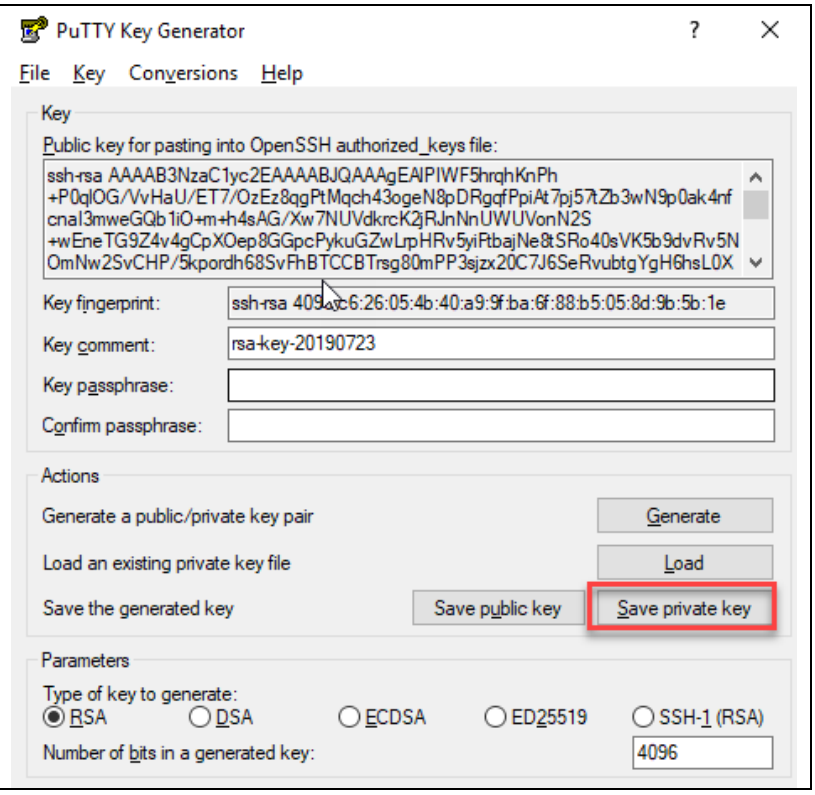
„Save public key“ anwählen



Dann, „Save private key“ anwählen

ACHTUNG : Der Private-Key darf NIE weiter gegeben werden !

Damit der Private-Key vor unberechtigten Gebrauch geschützt wird, ist seine Generierung mit einer Passphrase empfohlen. Man muss aber beachten, dass je nach eingesetzte Software eine Automatisierung der Anmeldung dadurch erschwert werden kann. In diesem Beispiel wird ohne Passphrase weitergefahren



2.3.2 Erstellen eines SSH-Schlüssel-Paares mit OpenSSH

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

Das Schlüssel-Paar kann zum Beispiel mit dem folgenden Befehl generiert werden:

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

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

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

3. Verbindung zu FDS

3.1 Einleitung

Der FDS-Server ist über die Adresse **fdsbc.post.ch** (Internet, Mietleitungen/IPSS) oder **fdsbc.pnet.ch** (Postnetz/DMZ der Post) erreichbar.

Unser SFTP Server läuft auf Standard-Port 22.

Der Benutzername sowie Details über Verzeichnisnamen, Dateinamen, Übermittlungszeiten, usw. wird im Rahmen der Service Bestellung kommuniziert.

Die geplanten Wartungsfenster werden auf https://www.post.ch/fds publiziert.

3.2 Test der Verbindung

Die Verbindung zu FDS kann zum Beispiel mittels *telnet* überprüft werden:

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

Achtung: es werden zwei IP-Adressen verwendet. Die beiden IP-Adressen können mittels DNS-Auflösung (nslookup fdsbc.post.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.

Falls der FDS Server nicht erreicht werden kann, muss überprüft werden, ob Ihr Firewall die Verbindung blockt.

Damit Informatik Post effizient helfen kann, ist es wichtig, die benötigten Informationen bereitzustellen (Benutzername, Fehlermeldung, genaue Zeit des Versuches, File- und Verzeichnisnamen)

4. FileZilla

4.1 Key Importieren mit FileZilla

Es können sowohl Keys in PUTTY- wie auch in OpenSSH-Format im FileZilla importiert werden.

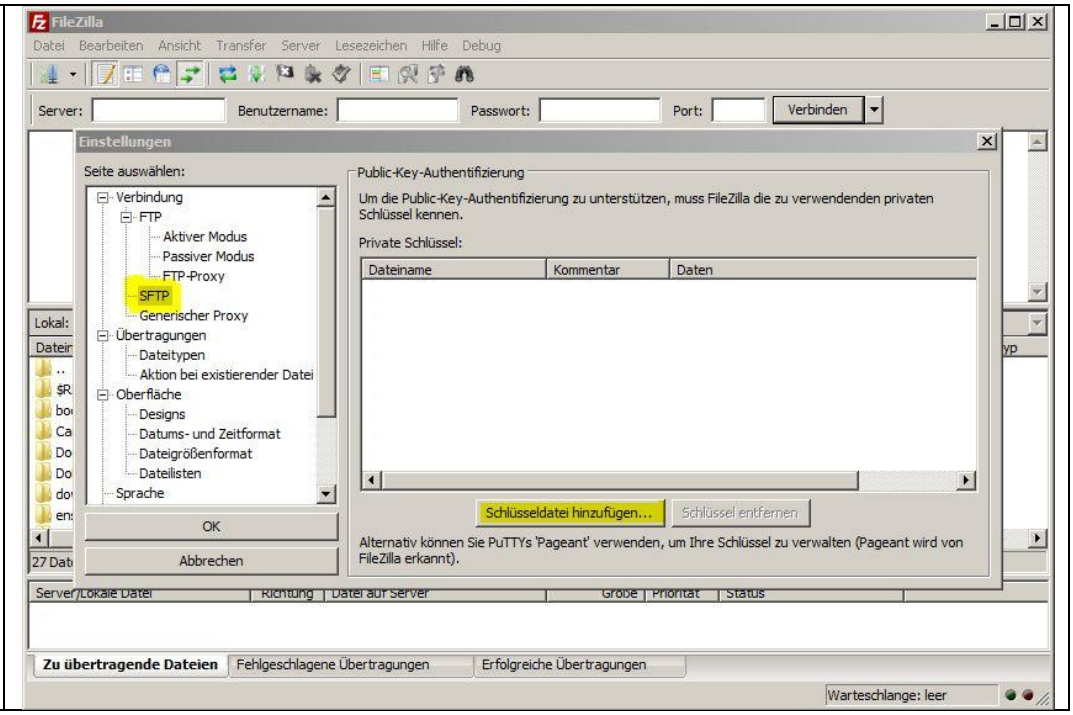
FileZilla starten

1) **Bearbeiten**
2) **Einstellungen** (Fenster geht auf)

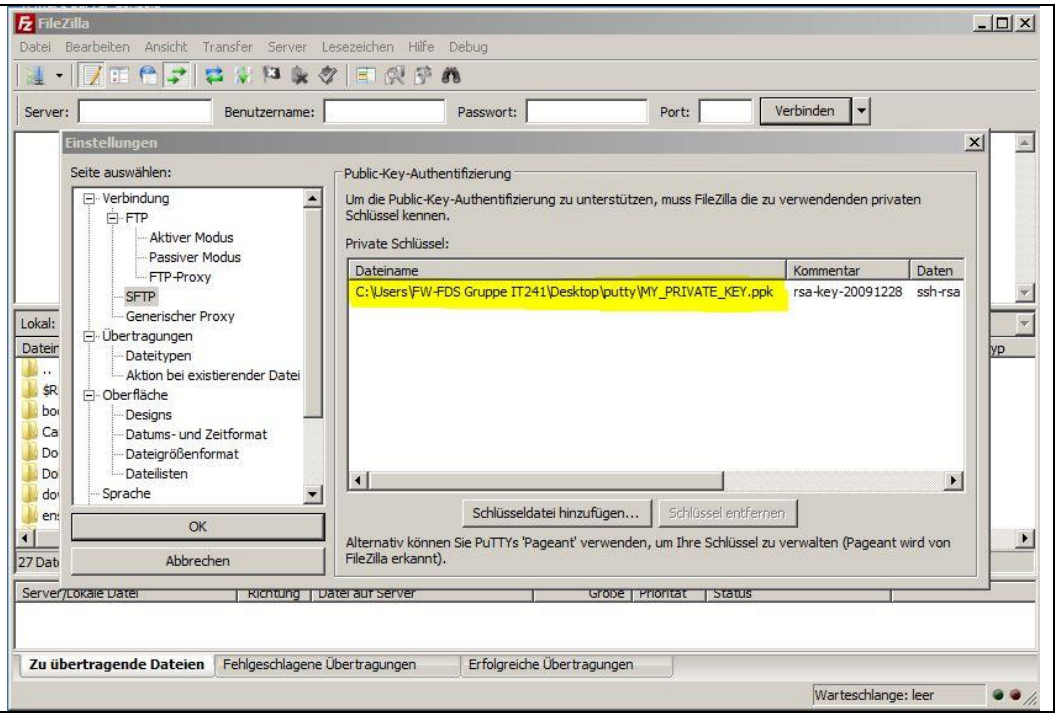
=> SFTP

=> Schlüsseldatei hinzufügen

(dann die korrekte Private-Key-Datei auswählen)

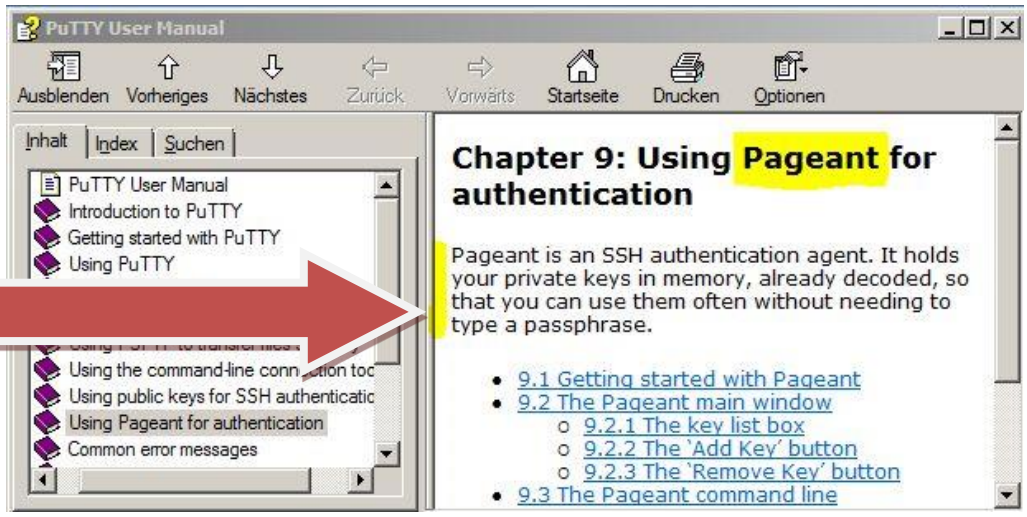


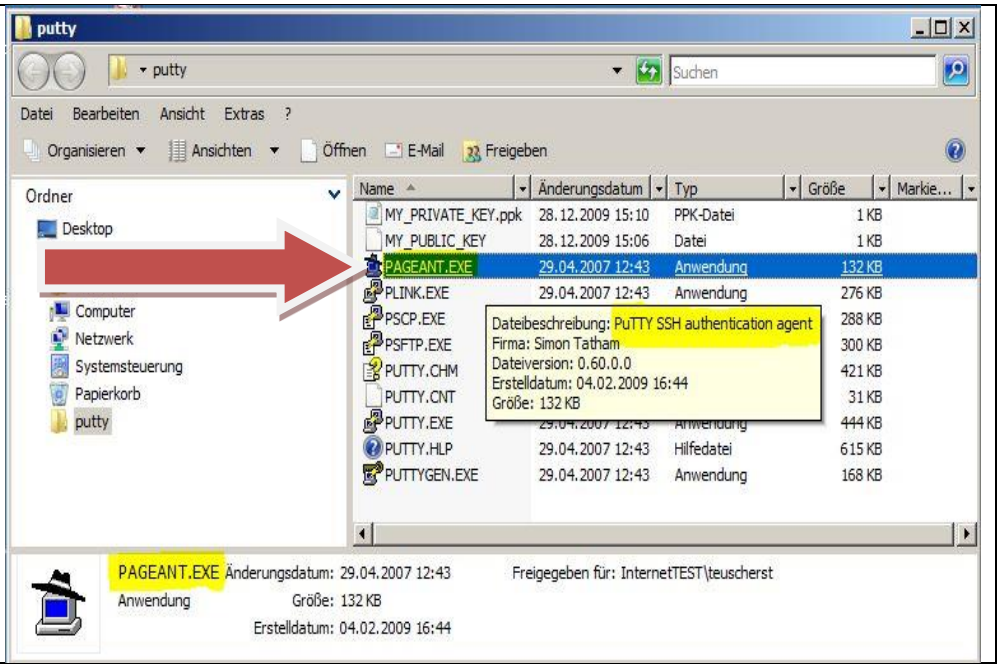
Diese (gelbe) Zeile zeigt dass der Key erfolgreich importiert wurde.



4.2 Automatisches Importieren mit PuTTY's Pageant

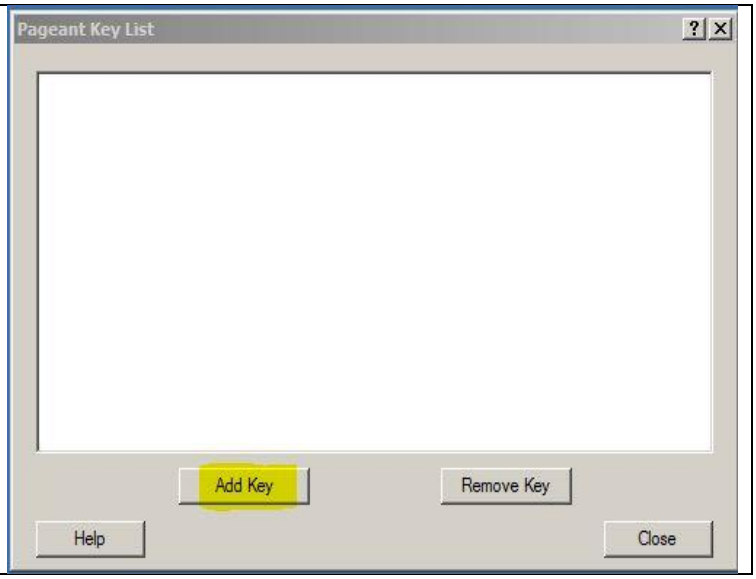
Der „Pageant" (PuTTY authentication agent) ist ein SSH-Agent mit dem SSH-Authentifizierungen weitergereicht werden können. Pageant kann Schlüssel laden und lokalen Programmen auf Anfrage zur Verfügung stellen. Die Schnittstelle ist offen, so dass sich weitere Programme an diesen Service von Pageant anbinden können.

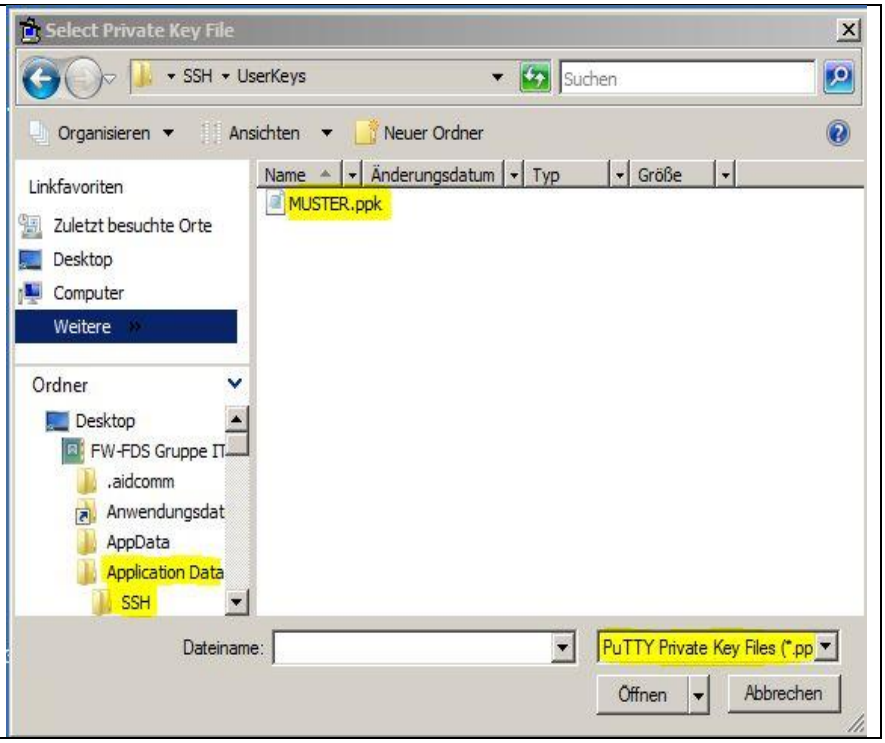


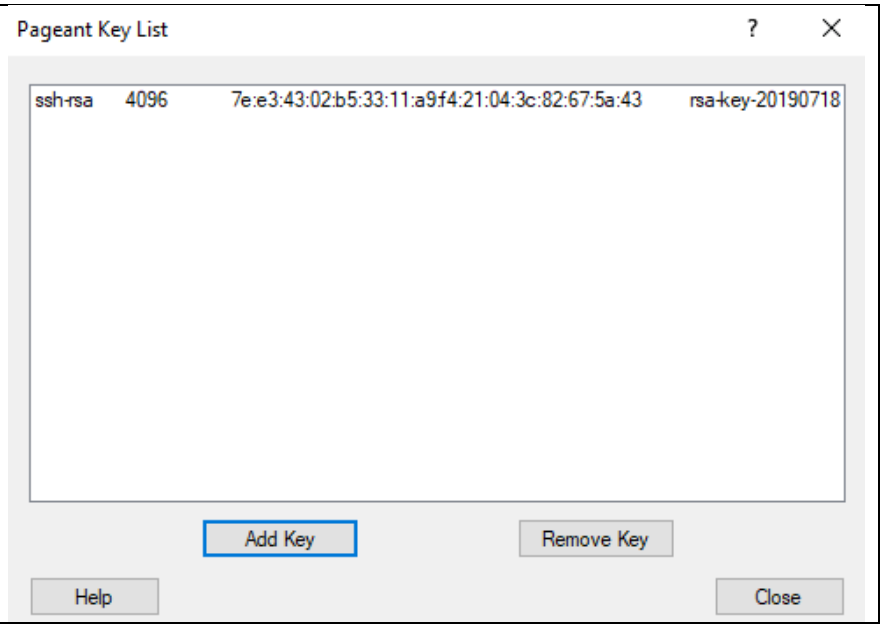
PAGEANT.EXE starten	

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

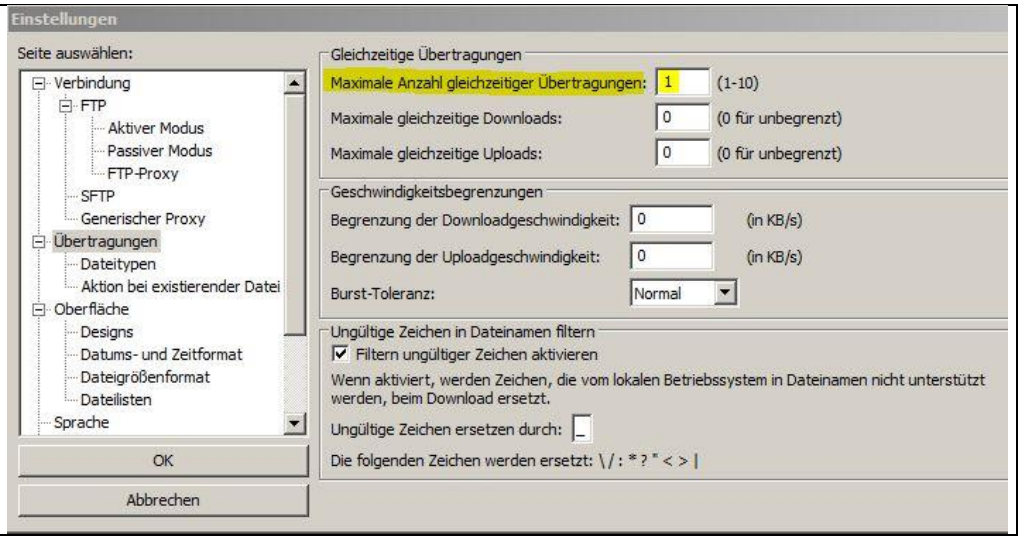
Dieses Icon erscheint in der Task-Bar :	

Doppelklick „auf Hut“ im System-Tray : Nach dem Öffnen erscheint das (noch) leere „Pageant-Key-List Fenster“ :	

Mit „Add Key“ den Private-Key auswählen und mit „Öffnen“ bestätigen. Hier wird nur das PuTTY-Format akzeptiert.	

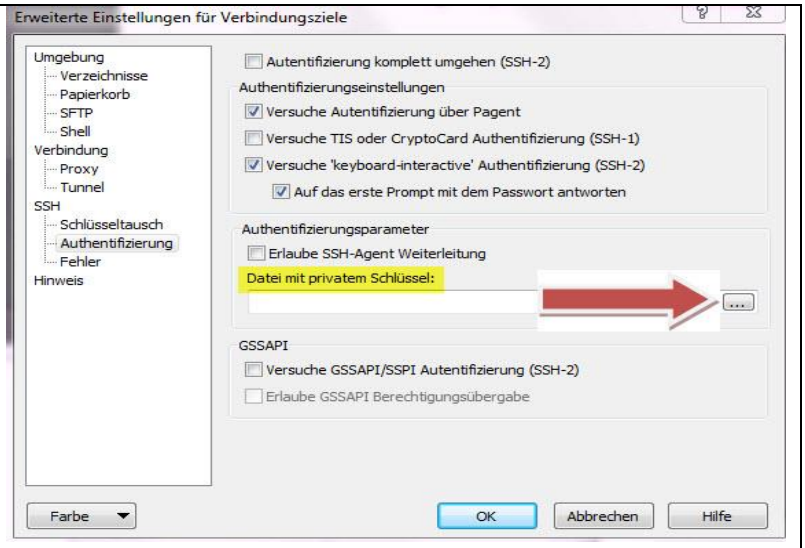
Zeigt sich der Key wie folgendes Beispiel, wurde er korrekt geladen und ist nun im Memory des PCs. Aus dem Memory haben diverse „SSH-Programme“ und vor allem FileZilla direkt Zugriff zum Key.	

4.3 Hinweise zu FileZilla

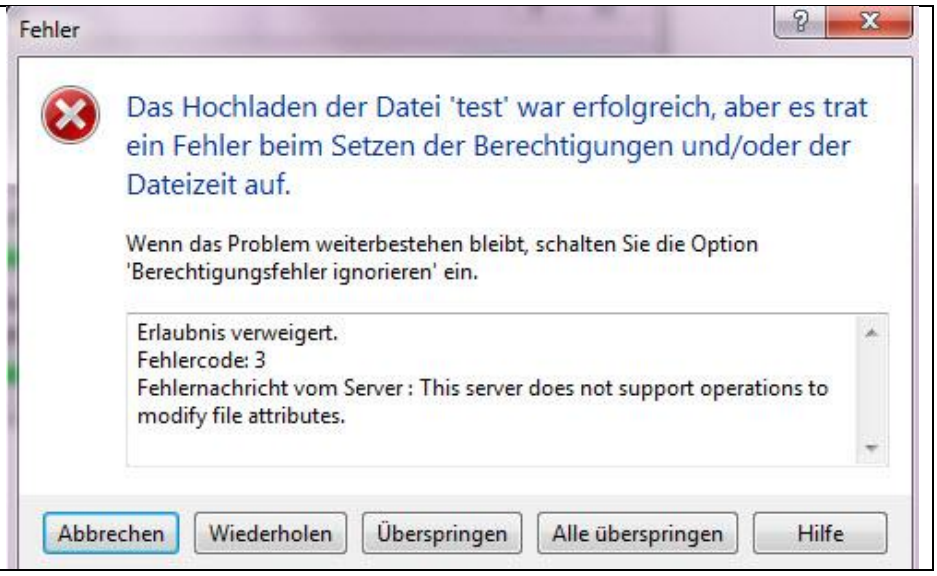
Die Post CH AG hat als eines seiner Schutzmechanismen auch ein IDS/IPS-System im Einsatz. Um nicht ausgesperrt zu werden empfehlen wir, die Anzahl gleichzeitiger Übertragungen auf eine oder maximal 3 zu begrenzen!	

5. WinSCP

5.1 Key Importieren mit WinSCP

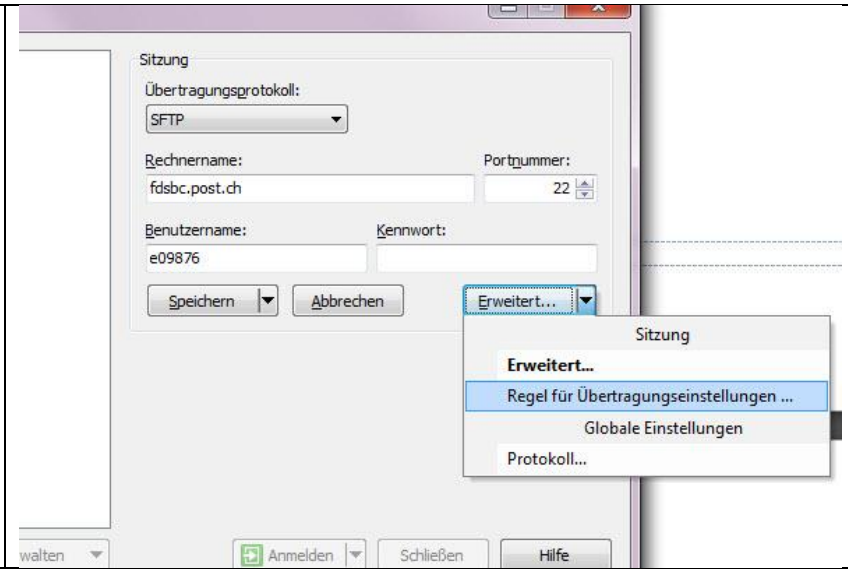
1) WinSCP starten 2) auf „Erweitert…“ klicken 3) auf „Authentifizierung“ klicken „Öffnen –Feld“ ➔ […] anklicken und den private Key auswählen !	

5.2 Hinweise zu WinSCP

Sollten Sie Probleme mit Berechtigungen nach dem Übertragen der Dateien haben …	

… so können Sie diese unter „Erweitert…“ …

„Regel für Übertragungseinstellungen …“



… beheben. ➔

=> aktivieren Sie die „Berechtigungsfehler ignorieren“ Option.