

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	4
1.1 Einleitung	4
1.2 Definitionen, Akronyme und Abkürzungen	4
2. SFTP.....	5
2.1 Einleitung	5
2.2 Sicherheit.....	5
2.2.1 Verschlüsselungs-Algorithmen	5
2.2.2 Message Authentication Codes (MAC)	5
2.3 Public-, und Private Key	6
2.3.1 Erstellen eines SSH-Schlüssel-Paares mit PuTTY	6
2.3.2 Erstellen eines SSH-Schlüssel-Paares mit OpenSSH	9
3. Verbindung zu FDS	10
3.1 Einleitung	10
3.2 Test der Verbindung	10
4. FileZilla.....	11
4.1 Key Importieren mit FileZilla	11
4.2 Automatisches Importieren mit PuTTY's Pageant.....	12
4.3 Hinweise zu FileZilla	14
5. WinSCP	15
5.1 Key Importieren mit WinSCP	15
5.2 Hinweise zu WinSCP.....	15

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 benutzten 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	<u>S</u> ecure <u>C</u> opy oder SCP ist ein Protokoll zur verschlüsselten Übertragung von Daten zwischen zwei Computern über ein Rechnernetz.
sftp	SFTP oder <u>S</u> SH <u>F</u> ile <u>T</u> ransfer <u>P</u> rotocol 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

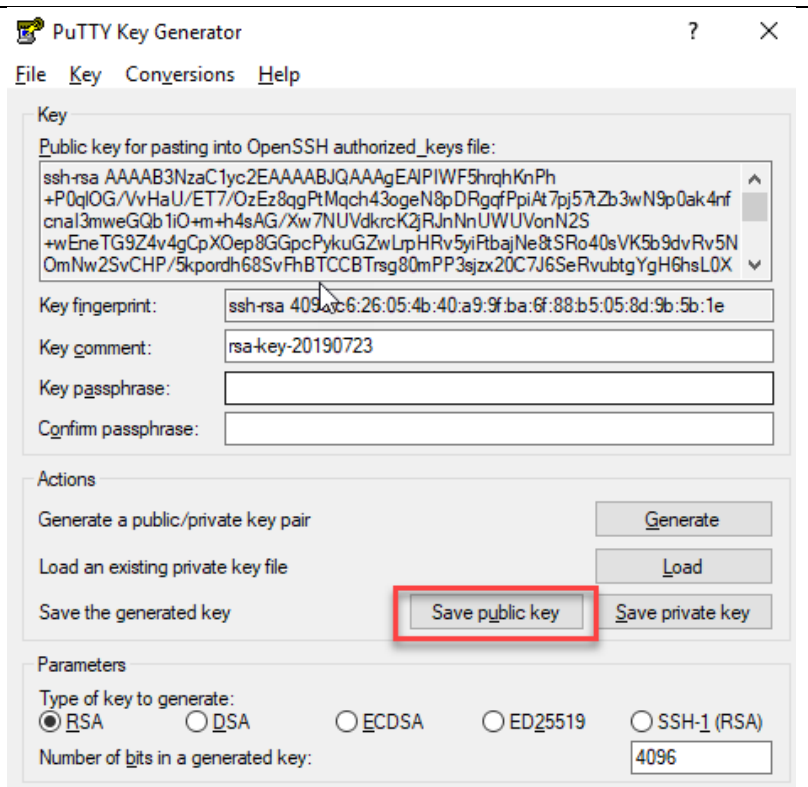
The screenshot shows the PuTTY Key Generator window. The 'Key' section displays 'No key.'. The 'Actions' section has buttons for 'Generate', 'Load', 'Save public key', and 'Save private key'. The 'Parameters' section shows 'Type of key to generate:' with radio buttons for RSA (selected), DSA, ECDSA, ED25519, and SSH-1 (RSA). The 'Number of bits in a generated key:' is set to 4096. Red boxes highlight the RSA radio button and the 4096 value in the bits field.

Maus-Cursor über die Fläche unter dem blauen Balken bewegen

The screenshot shows the PuTTY Key Generator window. The 'Key' section displays 'Please generate some randomness by moving the mouse over the blank area.' with a green progress bar. The 'Actions' section has buttons for 'Generate', 'Load', 'Save public key', and 'Save private key'. The 'Parameters' section shows 'Type of key to generate:' with radio buttons for RSA (selected), DSA, ECDSA, ED25519, and SSH-1 (RSA). The 'Number of bits in a generated key:' is set to 4096. A mouse cursor is positioned over the green bar.

Wenn fertig, erscheint die Maske mit den Keys.

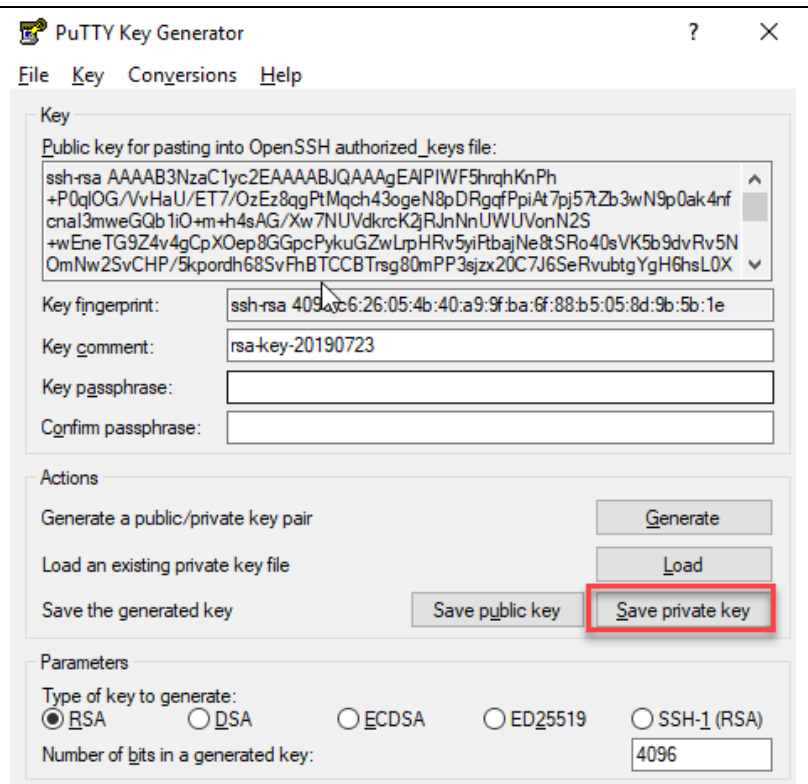
„Save public key“ anwählen



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 --- >
ACdBLStDxIURm03gmMcBhKHDq4owQ1DyESva0LWhIaxFwHpzamOAbPYVqBMbqT38
Bc1eG10EE4d3yyWoMLOpwsbhbmjSUjVV4JeDpNciqADBK5mQ3HNGNyKNqQ=
-----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 AAAAB3NzaC1yc2EAAAADAQAB < --- SNIP --- > 6mE05Gh28Vw== 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

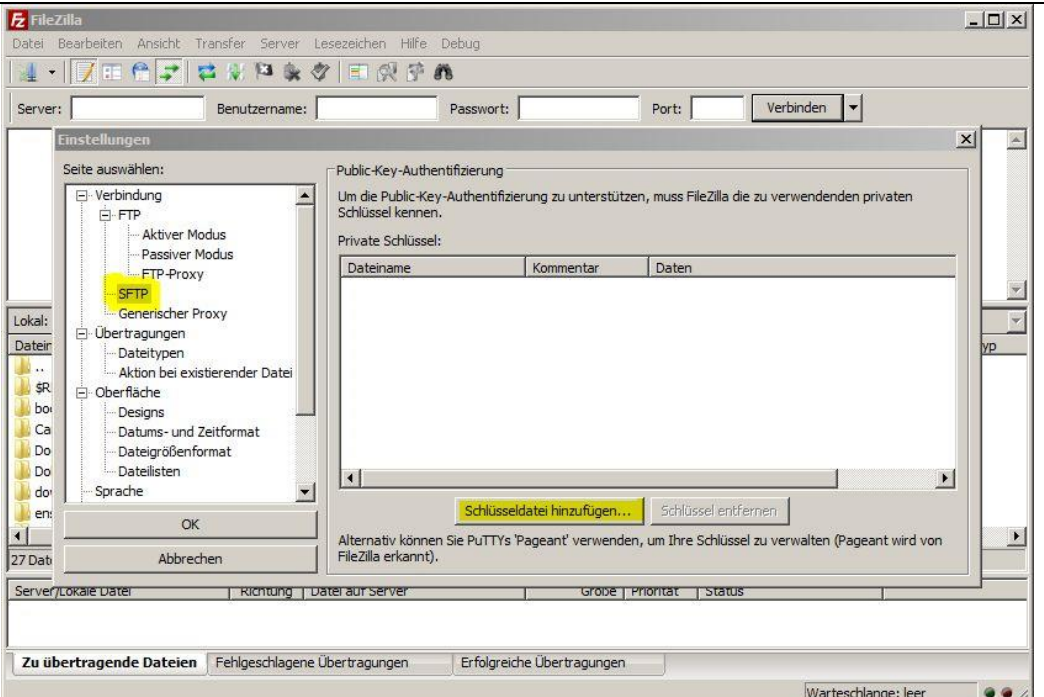
Es können sowohl Keys in PUTTY- wie auch in OpenSSH-Format im FileZilla importiert werden.

FileZilla starten

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

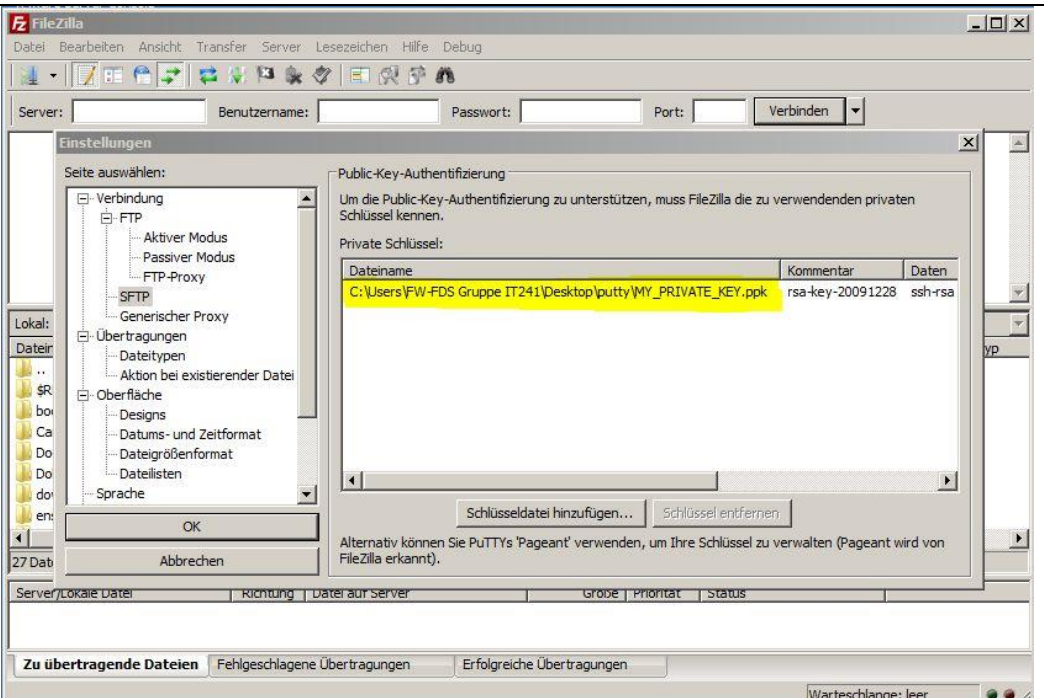
=> SFTP

=> Schlüsseldatei hinzufügen
(dann die korrekte Private-Key-Datei auswählen)



The screenshot shows the FileZilla 'Einstellungen' (Settings) dialog box. The 'Verbindung' (Connection) section is expanded, and 'SFTP' is highlighted in yellow. The 'Public-Key-Authentifizierung' (Public-Key Authentication) section is also visible, with a note that FileZilla needs to know the private key used for authentication. Below this, there is a table for 'Private Schlüssel:' (Private Keys) with columns for 'Dateiname' (Filename), 'Kommentar' (Comment), and 'Daten' (Data). The table is currently empty. At the bottom of this section, there are buttons for 'Schlüsseldatei hinzufügen...' (Add key file...) and 'Schlüssel entfernen' (Remove key). The 'OK' and 'Abbrechen' (Cancel) buttons are at the bottom of the dialog.

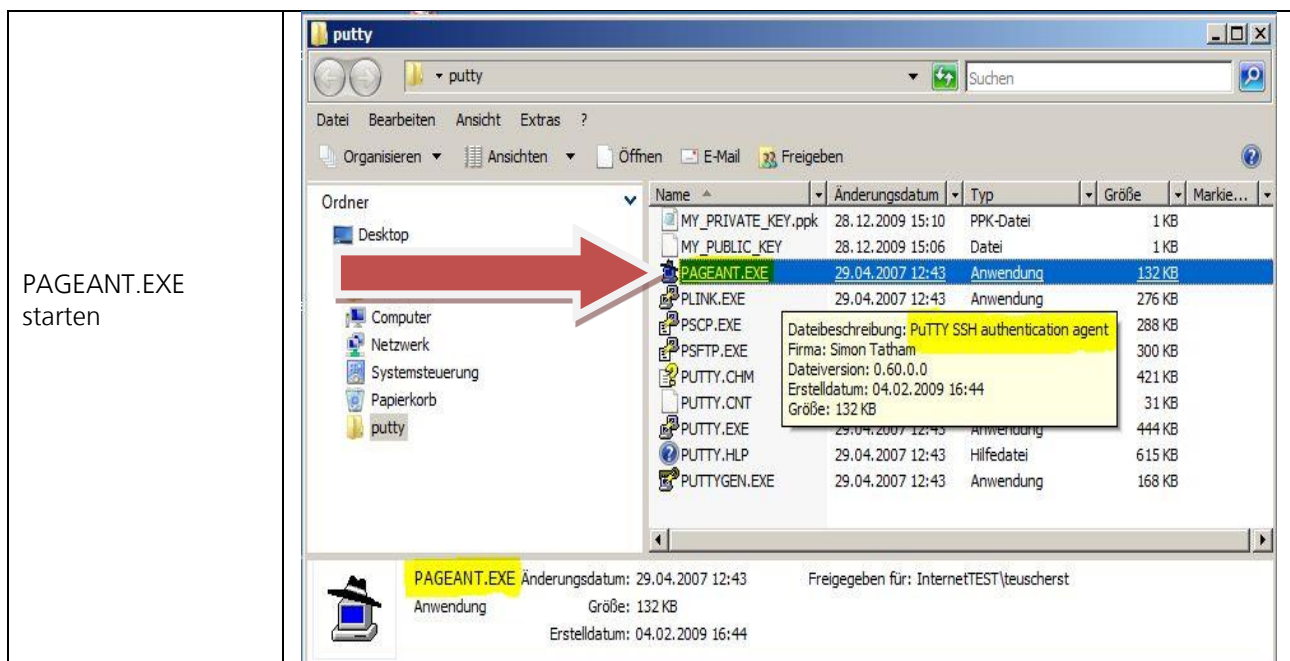
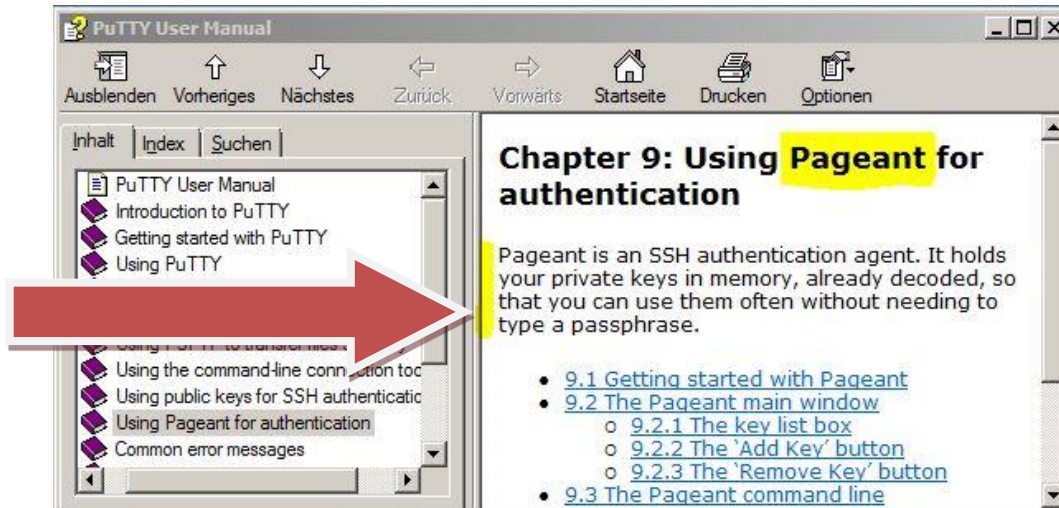
Diese (gelbe) Zeile zeigt dass der Key erfolgreich importiert wurde.



The screenshot shows the FileZilla 'Einstellungen' (Settings) dialog box, similar to the previous one. In the 'Private Schlüssel:' table, there is now one entry highlighted in yellow. The entry is: 'C:\Users\FW-FDS Gruppe IT241\Desktop\putty\MY_PRIVATE_KEY.ppk' in the 'Dateiname' column, 'rsa-key-20091228' in the 'Kommentar' column, and 'ssh-rsa' in the 'Daten' column. The 'OK' and 'Abbrechen' (Cancel) buttons are at the bottom of the dialog.

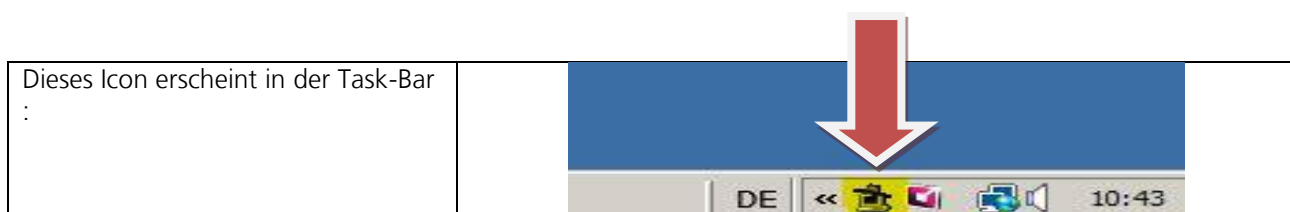
4.2 Automatisches Importieren mit PuTTY's Pageant

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

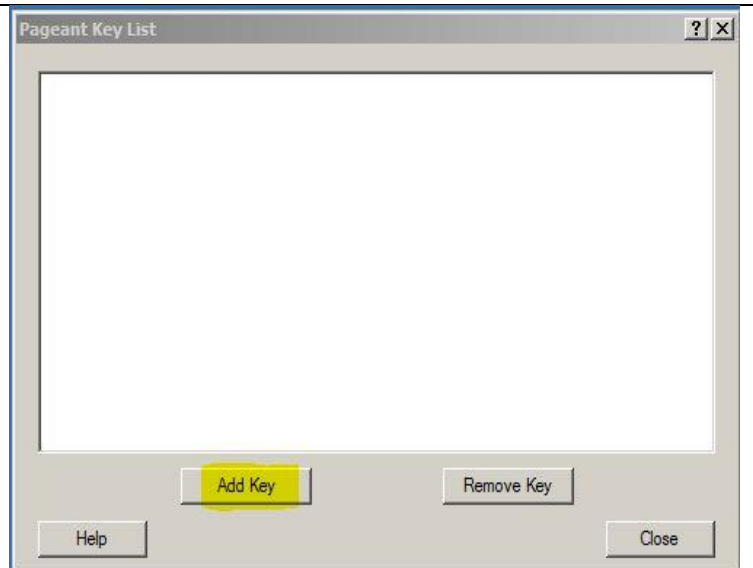
Pageant nistet sich im System-Tray rechts unten in der Schnellstart-Leiste ein und zeigt alle in Pageant gespeicherten Sessions an.



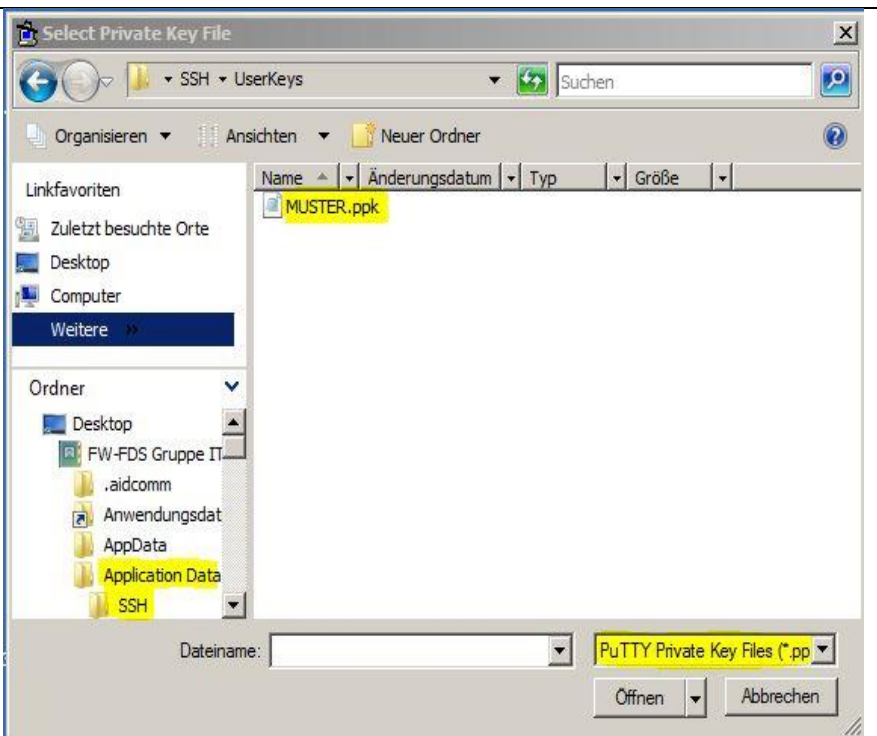
Dieses Icon erscheint in der Task-Bar
:

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.

Key Type	Key Size	Key Fingerprint	Key Name
ssh-rsa	4096	7e:e3:43:02:b5:33:11:a9f4:21:04:3c:82:67:5a:43	rsa-key-20190718

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!

Einstellungen

Seite auswählen:

- Verbindung
 - FTP
 - Aktiver Modus
 - Passiver Modus
 - FTP-Proxy
 - SFTP
 - Generischer Proxy
- Übertragungen**
 - Dateitypen
 - Aktion bei existierender Datei
- Oberfläche
 - Designs
 - Datums- und Zeitformat
 - Dateigrößenformat
 - Dateilisten
- Sprache

Gleichzeitige Übertragungen

Maximale Anzahl gleichzeitiger Übertragungen: (1-10)

Maximale gleichzeitige Downloads: (0 für unbegrenzt)

Maximale gleichzeitige Uploads: (0 für unbegrenzt)

Geschwindigkeitsbegrenzungen

Begrenzung der Downloadgeschwindigkeit: (in KB/s)

Begrenzung der Uploadgeschwindigkeit: (in KB/s)

Burst-Toleranz:

Ungültige Zeichen in Dateinamen filtern

Filtern ungültiger Zeichen aktivieren

Wenn aktiviert, werden Zeichen, die vom lokalen Betriebssystem in Dateinamen nicht unterstützt werden, beim Download ersetzt.

Ungültige Zeichen ersetzen durch:

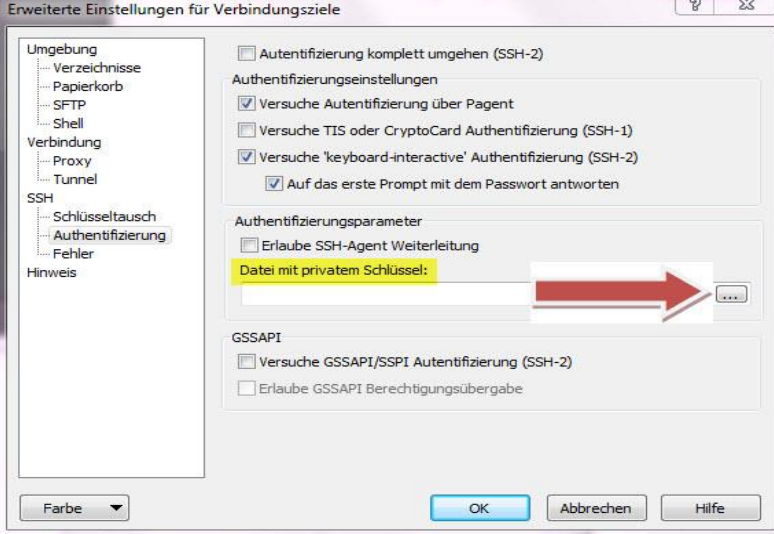
Die folgenden Zeichen werden ersetzt: \ / : * ? " < > |

OK

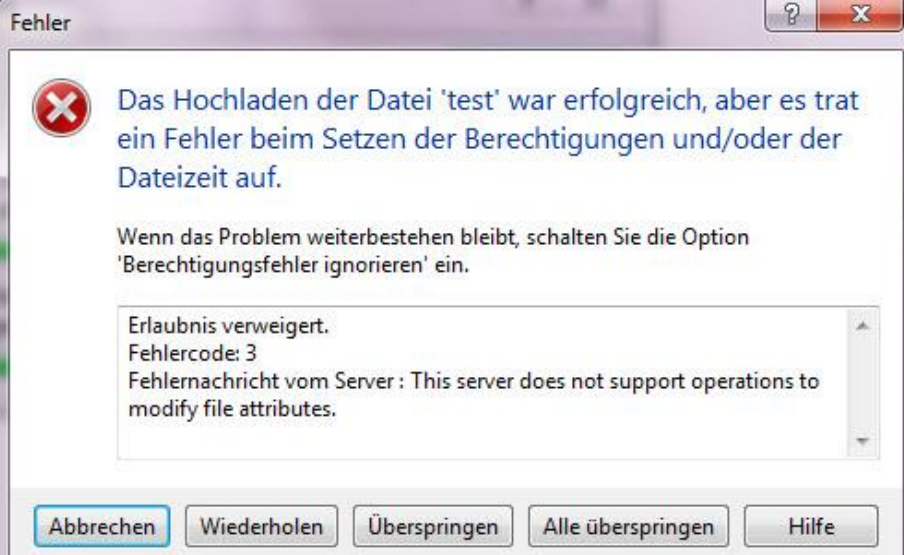
Abbrechen

5. WinSCP

5.1 Key Importieren mit WinSCP

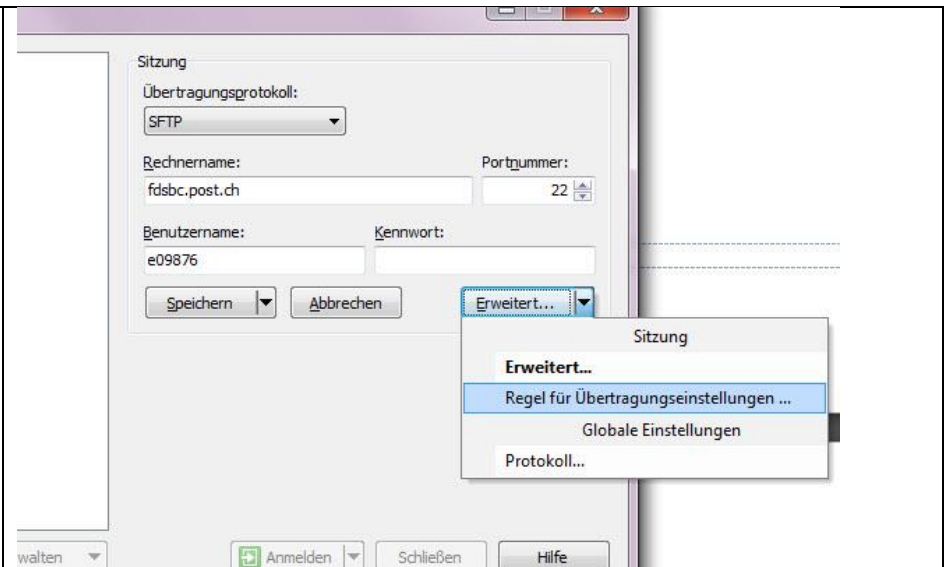
<p>1) WinSCP starten</p> <p>2) auf „Erweitert...“ klicken</p> <p>3) auf „Authentifizierung“ klicken</p> <p>„Öffnen -Feld“ → [...] anklicken und den private Key auswählen !</p>	
--	--

5.2 Hinweise zu WinSCP

<p>Sollten Sie Probleme mit Berechtigungen nach dem Übertragen der Dateien haben ...</p>	
--	--

... so können Sie diese unter „Erweitert...“ ...

„Regel für Übertragungseinstellungen ...“



... beheben. →

=> aktivieren Sie die „Berechtigungsfehler ignorieren“ Option.

