

DOKUMENTATION

Sichere Verbindung zum
dbh Fileserver



Version 1.3

© 25.11.2019 dbh Logistics IT AG

Eine Weitergabe des Handbuchs an Dritte ist strengstens untersagt.

dbh Logistics IT AG

Martinistr. 47-49

28195 Bremen

IT Services ■ Customer Support

Ansprechpartner bei Rückfragen: Customer Service

Servicezeiten: Mo. - Fr. 8:00 - 18:00 Uhr

Tel. +49 421 30902-22

support@dbh.de

VERSIONSÜBERSICHT

Datum	Version	Änderung	Autor
09.10.2018	1.0	Anpassung der Bilder und des Textes auf den aktuellen Stand	NPo
10.10.2018	1.1	Kleine Ergänzungen durchgeführt	SSc
11.10.2018	1.2	Ansprechpartner und Tel. Nummer angepasst	NPo
25.11.2019	1.3	Punkt 6 ist veraltet und wurde entfernt	Nih

Welche Inhalte haben sich zur letzten Version geändert?

Welche Inhalte sind neu in der aktuellen Version?

Der dbh Fileserver dient zum Austausch von Importdateien von dbh Applikationen, die im dbh Logistics IT AG Rechenzentrum betrieben werden. Die dbh Applikationen werden in einem eigenen Netzsegment betrieben. Zugänge über das Internet (sowohl für den Dateiaustausch als auch für die Zugänge über den Webserver) stehen in der DMZ.

Damit die Dateiübertragung gesichert gegenüber den anderen Informationsflüssen im Internet stattfinden kann, muss zuvor eine sichere Verbindung zwischen den Beteiligten aufgebaut werden. Der Datentransfer zur dbh erfolgt durch SFTP mit Public-Key Authentifizierung.

Im Folgenden wird beschrieben, wie diese gesicherte Verbindung einzurichten ist.

INHALT

1	Einleitung.....	1
2	Was wird gebraucht?.....	1
2.1	Username/Passwort	1
2.2	Public Key	1
3	Installation/Konfiguration.....	2
4	Benutzung.....	2
4.1	Dateiübertragung mit OpenSSH unter Unix	2
	Public Key	2
	Batchbetrieb	2
	Aufruf	2
4.2	Dateiübertragung mit Putty	2
	Public Key	3
	Batchbetrieb	3
	Aufruf	3
5	Verzeichnisse	4
6	Firewall Einstellungen.....	4
7	Anhang.....	4
7.1	Anhang A: OpenSSH unter UNIX/LINUX	4
	Public Key	4
7.2	Anhang C: Putty unter Windows	5
	Public Key	6

8	SICHERHEITSHINWEIS!	9
	Konfiguration Putty	9

1 Einleitung

SSH ist eine Protokoll Suite, die Verschlüsselung für Netzwerkdienste bereitstellt, wie etwa „remote Login“, also Einloggen auf einem anderen, entfernten Rechner, oder auch Datenübertragung von oder zu einem „remote“ Rechner.

Features:

- Starke Verschlüsselung
- X11 Forwarding (verschlüsselt X Window System Netzwerkverkehr)
- Port Forwarding (verschlüsselte Kanäle für bestimmte Protokolle)
- Starke Authentifizierung (Public Key, Einmal-Passwort und Kerberos Authentifizierung)
- Interoperabilität (arbeitet kompatibel zu den SSH 1.3, 1.5 und 2.0 Protokoll Standards)
- Datenkompression

2 Was wird gebraucht?

SSH client (SSH Version 2) für Unix oder Windows mit Filetransfer Support (SFTP)

Freie Lösung

Linux, UNIX: -Openssh (<https://www.openssh.com>)

Windows: -Putty (<https://www.chiark.greenend.org.uk/~sgtatham/putty>)

-WinSCP (<https://winscp.net/eng/index.php>) für Grafisches Interface

2.1 Username/Passwort

Die Authentifizierung erfolgt durch Eingabe des Benutzernamens und des Passwortes.

2.2 Public Key

Die Authentifizierung erfolgt mittels eines Public/Private Key Paares, wobei der Public Key serverseitig hinterlegt wird. Dies ermöglicht eine Anmeldung ohne Eingabe eines Passwortes. Wenn automatische Batch Prozesse zum Einsatz kommen sollen, ist dieses Verfahren zwingend erforderlich. Die Konfiguration des Public Key Verfahrens ist auf allen Plattformen grundsätzlich gleich.

-Erzeugung der Public/Private Keys

-Übertragung des Public Keys auf den Fileserver.

3 Installation/Konfiguration

Im Anhang werden die unterschiedlichen Produkte beschrieben:

-OpenSSH unter UNIX/LINUX (ANHANG A)

-Putty (Anhang C)

4 Benutzung

4.1 Dateiübertragung mit OpenSSH unter Unix

Public Key

```
$ sftp user@fx.dbh.de
sftp> put Datei1 Datei2 ...
sftp> get Datei1 Datei2 ...
```

Die Dateien werden ohne Eingabe eines Passwortes übertragen.

Batchbetrieb

Der Batchbetrieb kann mit einer Kommandodatei realisiert werden. In diese Datei werden SFTP Kommandos eingetragen die dann abgearbeitet werden:

```
z.B. >batch.txt put *.xml
      >quit
```

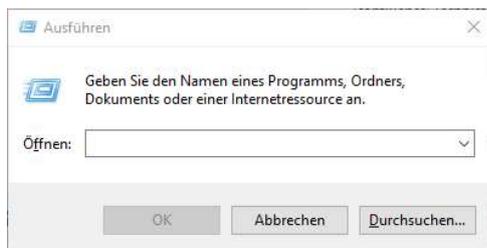
Überträgt alle xml Dateien aus dem lokalen Verzeichnis in das home Verzeichnis des Remote Systems.

Aufruf

```
C:\ sftp -b batch.txt user@fx.dbh.de
C:\
```

4.2 Dateiübertragung mit Putty

Die Dateiübertragung an den Fileserver erfolgt mit dem Programm „psftp“. Mit „Rechtsklick auf start -> Ausführen“ (Tastenkombination „Win“ + „R“) wird ein Eingabefenster gestartet. Hier muss nun nach "psftp" gesucht werden.



Public Key

```
C:\ psftp -i mykey.ppk user@fx.dbh.de
Using username "user".
Remote working directory ist /home/user
psftp> get Datei

psftp> put Datei1 Datei2 ...
psftp> quit
C:\
```

Die Dateien werden ohne Eingabe eines Passwortes übertragen.

Batchbetrieb

Der Batchbetrieb kann mit einer Kommandodatei realisiert werden. In diese Datei werden SFTP Kommandos eingetragen die dann abgearbeitet werden:

```
z.B. >batch.txt put *.xml
      >quit
```

Überträgt alle xml Dateien aus dem lokalen Verzeichnis in das home Verzeichnis des Remote Systems.

Aufruf

```
C:\ psftp -b batch.txt user@fx.dbh.de
C:\
```

Es können alle sftp Kommandos in der Kommando Datei verwendet werden.

```
C:\Programme\PUTTY>psftp
psftp: no hostname specified; use "open host.name" to conne
psftp> help
! run a local command bye finish
your SFTP session
cd change your remote working directory chmod
change file permissions and modes
close finish your SFTP session but do not quit PSFTP
del delete files on the remote server dir list
remote files exit finish your SFTP session
get download a file from the server to your local
machin help give help lcd change local working
directory lpwd print local working directory ls
list remote files
mget download multiple files at once mkdir
create directories on the remote server
mput upload multiple files at once mv move
or rename file(s) on the remote server open
connect to a host
put upload a file from your local machine to the
server pwd print your remote working directory quit
finish your SFTP session reget continue downloading
files
ren move or rename file(s) on the remote
server reput continue uploading files rm
delete files on the remote server rmdir
remove directories on the remote server
psftp>
```

5 Verzeichnisse

Auf dem dbh Fileserver werden für den Datenaustausch standardmäßig pro User zwei Verzeichnisse (import und export) angelegt. Die Daten, die zum dbh Fileserver übertragen werden, müssen in "import" abgelegt werden. Daten für den Transfer zum Kunden werden in „export“ bereitgestellt. Nach der erfolgreichen Übertragung müssen die Dateien im „export“-Verzeichnis gelöscht oder in ein Unterverzeichnis verschoben werden.

6 Firewall Einstellungen

Für die SFTP Kommunikation muss eine ausgehende Verbindung auf fx.dbh.de (194.99.88.17) Port 22 freigegeben sein.

7 Anhang

7.1 Anhang A: OpenSSH unter UNIX/LINUX

Installation von OpenSSH nach Installationsanweisung.

Public Key

Zur Erzeugung des Public/Private Key Paares dient der Befehl "ssh-keygen".

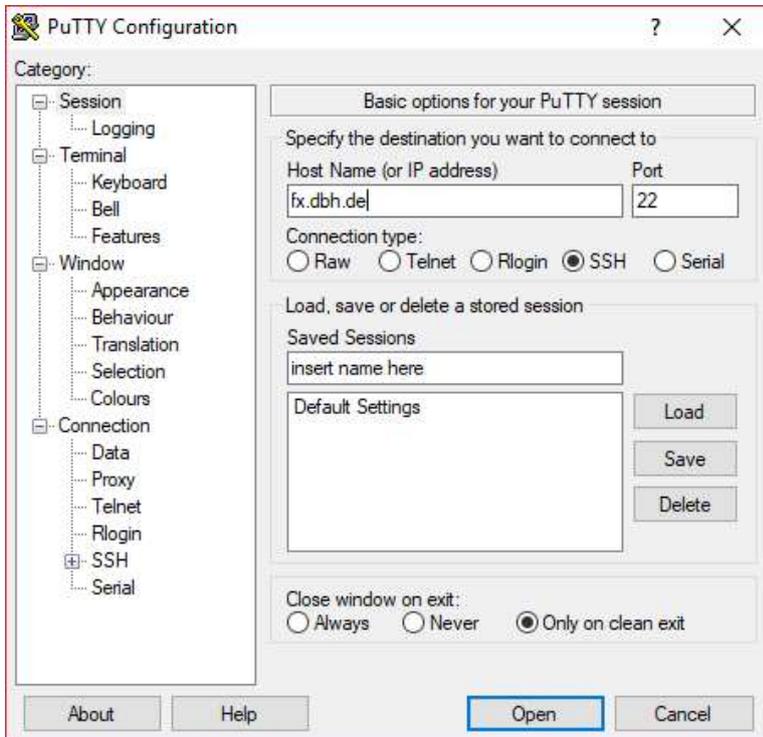
```
$ ssh-keygen -t rsa -b 2048 <RETURN>
$ Generating public/private dsa key pair.
$ Enter file in which to save the key (/homedir/.ssh/id_rsa):<RETURN>
Enter passphrase (empty for no passphrase):<RETURN>
Enter same passphrase again: <RETURN>
Your identification has been saved in /homedir/.ssh/id_rsa.
Your public key has been saved in /homedir/.ssh/id_rsa.pub.
The key fingerprint is:
.
.
.
```

Bei der Aufforderung eine Passphrase einzugeben bitte NICHTS eingeben, sondern nur zweimal mit <RETURN> bestätigen. Im Verzeichnis „/homedir/.ssh/“ befindet sich nun die Datei „id_rsa.pub“

Diese Datei wird per Email an <mailto:support@dbh.de> geschickt und dann auf dem SFTP-Server eingerichtet.

7.2 Anhang C: Putty unter Windows

Download des Installerpaketes unter <https://the.earth.li/~sgtatham/putty/0.70/w32/> . Hier kann die neueste Version runtergeladen werden (putty-'Versionsnummer'-installer.msi) Installation mit Doppelklick starten. Nach erfolgter Installation Putty starten.

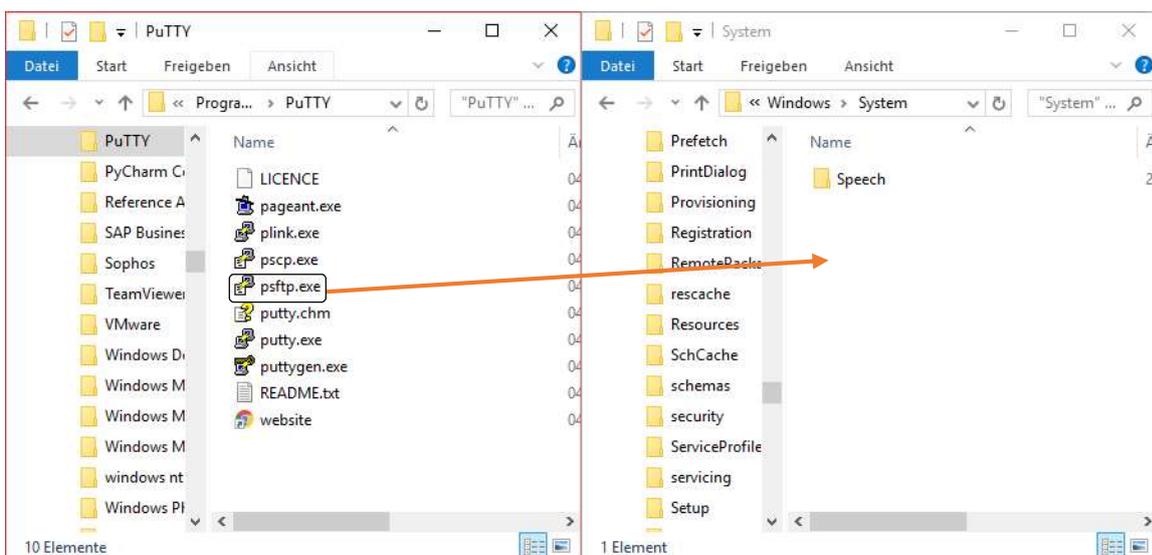


-Unter „Host Name (or IP address)“ den Servernamen (fx.dbh.de) eintragen.

-Bei „Connection type“ „SSH“ auswählen.

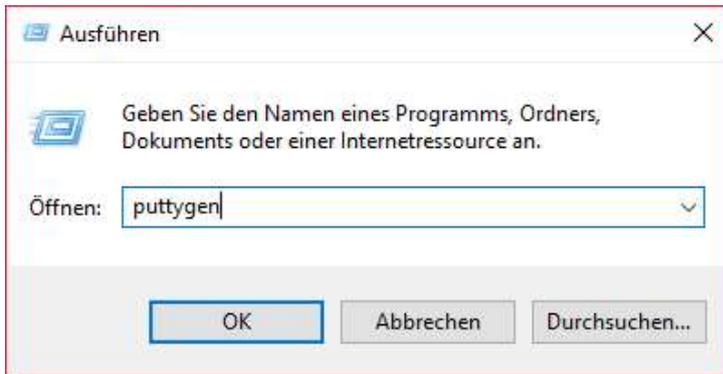
-Unter „Saved sessions“ einen beliebigen Namen für die Session vergeben. Mit „Save“ abspeichern.

-Aus dem Programmordner von Putty (idR. „C:\Program Files (x86)\PuTTY“) die Datei „psftp.exe“ nach „C:\Windows\System“ kopieren.

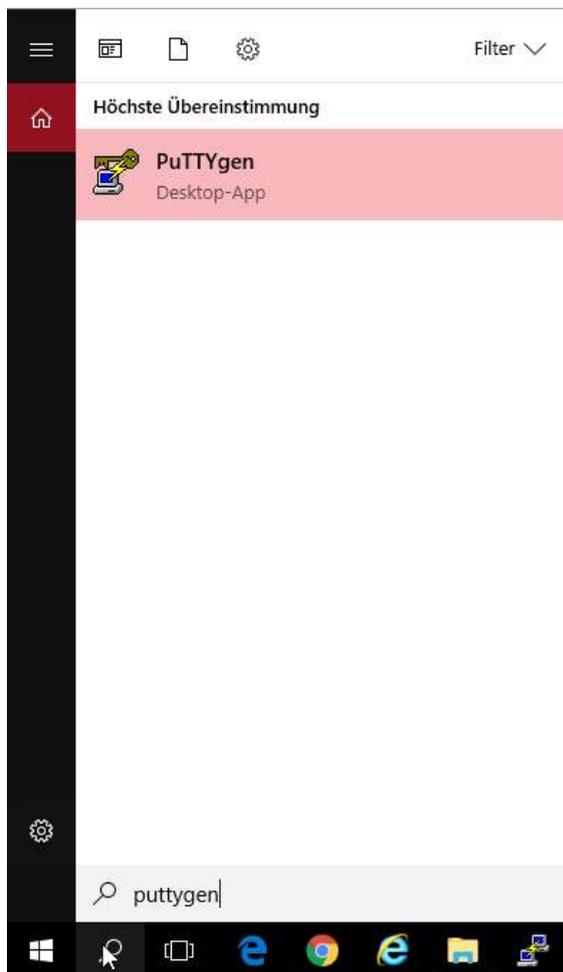


Public Key

Nach der erfolgten Installation (s.o.) des Programmpaketes muss zunächst ein Schlüsselpaar erzeugt werden.

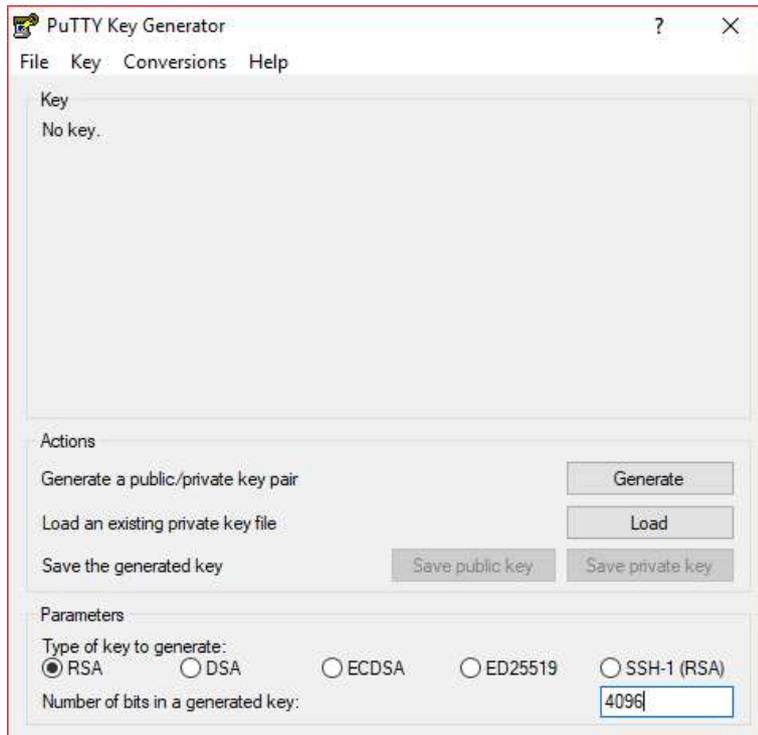


Mit „Rechtsklick auf Start -> Ausführen“ (Tastenkombination „Win“ + „R“) wird ein Eingabefenster gestartet. Dort geben Sie „puttygen“ ein und drücken „Enter“.



In der Windows Suchleiste nach "puttygen" suchen und dieses starten.

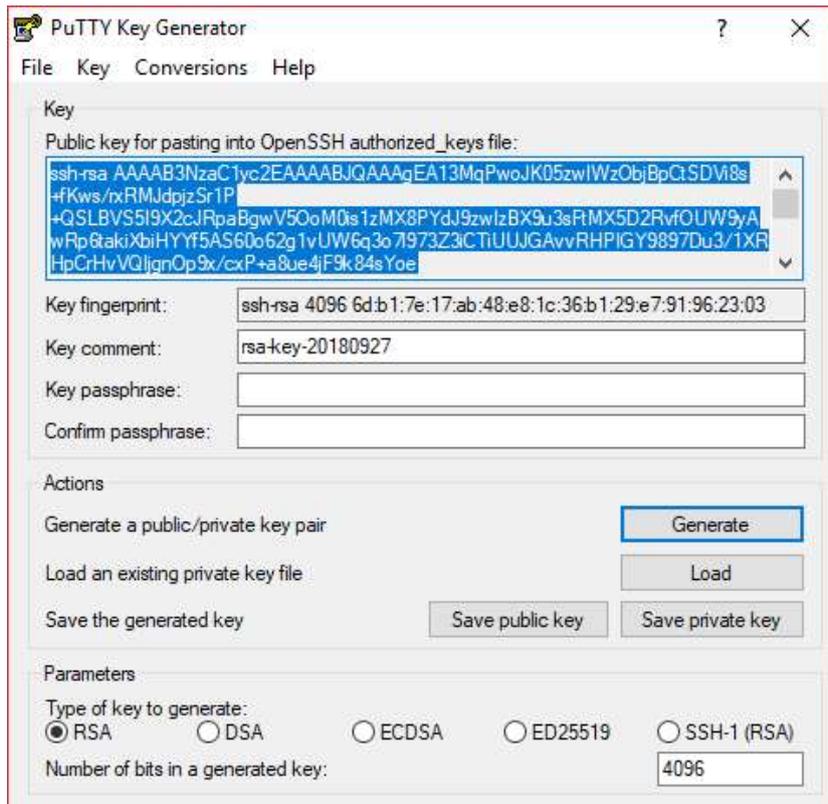
Unter „Type of key to generate“ „RSA“ auswählen und bei Number of bits in a generated key“ „4096“ eintragen.



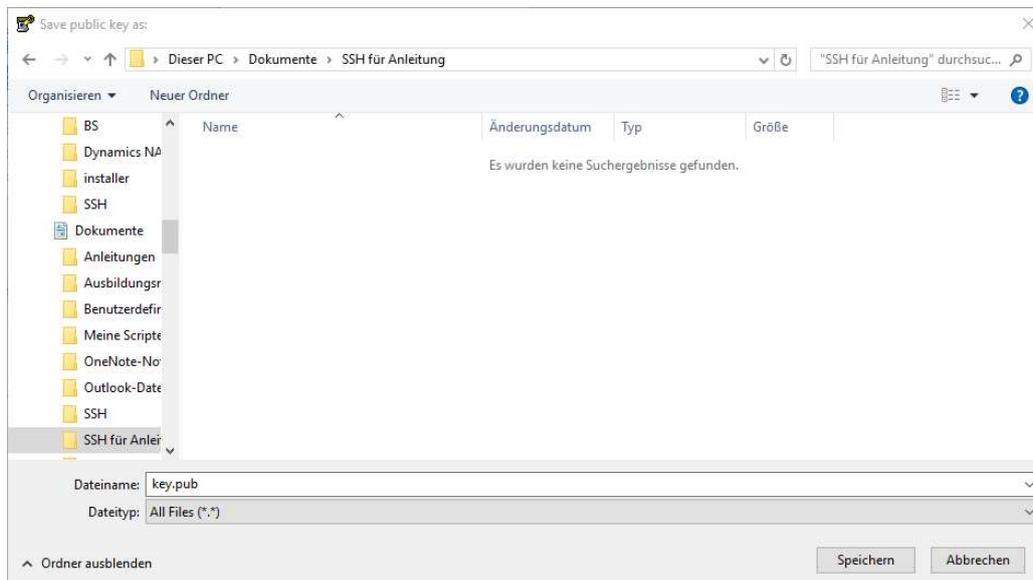
Mit „Generate“ den Vorgang starten, dabei die Maus willkürlich über die freie Fläche bewegen, bis der Ladebalken durchgelaufen ist.



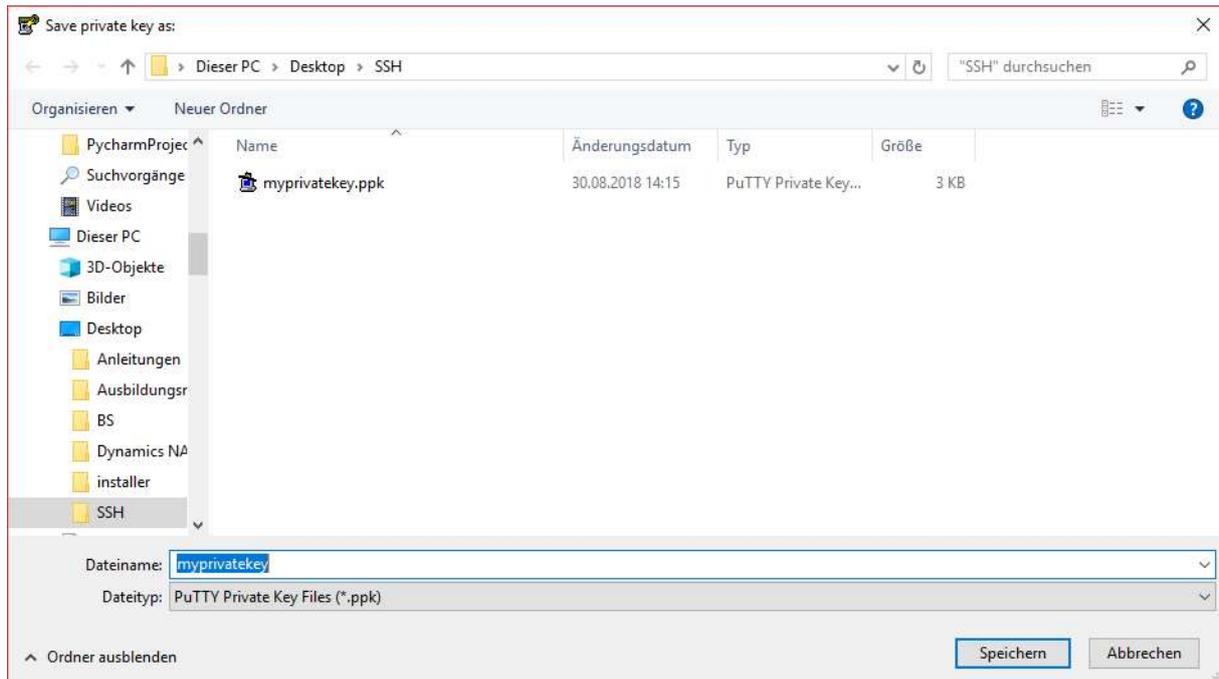
Die Erzeugung des Schlüsselpaares dauert einen kleinen Moment.



Mit einem Klick auf "Save public key" speichert man nun den Public Key.



Anschließend mit „Save private key“ den Private Key speichern. Hierbei taucht eine Warnung auf, welche mit „Ja“ zu beantworten ist.



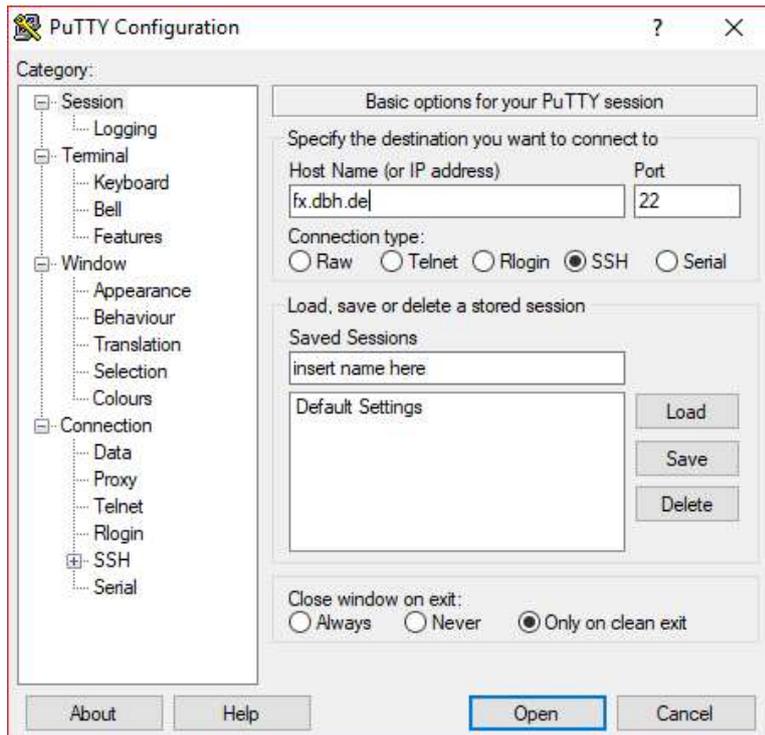
8 SICHERHEITSHINWEIS!

Das Abspeichern des Private Keys ohne Passphrase stellt ein potentielles Sicherheitsrisiko dar. Es ist durch geeignete Maßnahmen (Zugriffsberechtigung) sicherzustellen, dass nur berechtigte Personen Zugriff auf den Private Key haben.

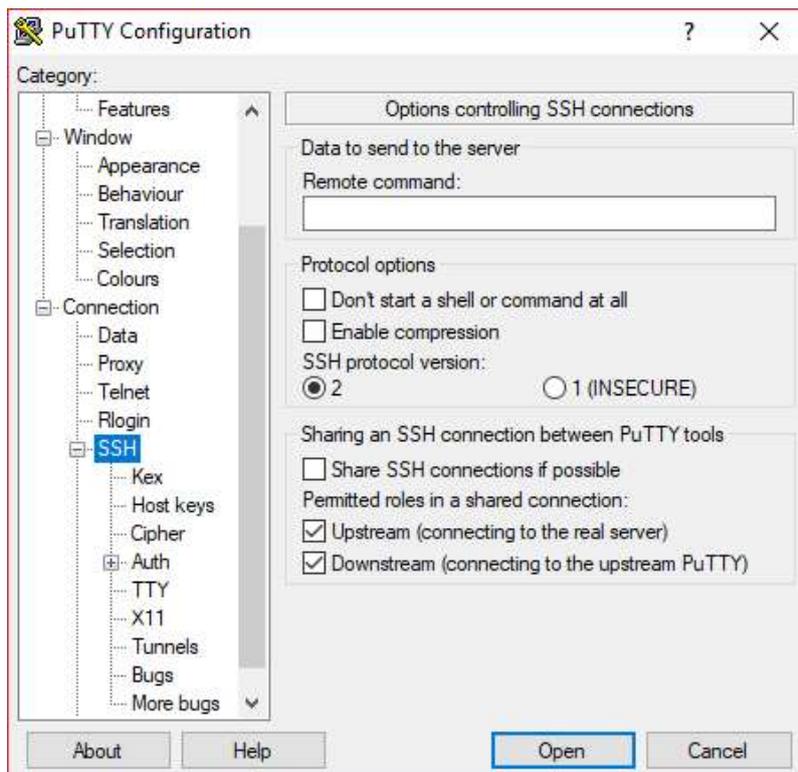
Die Datei mit dem Public Key (key.pub) wird per Email an support@dbh.de geschickt und dann auf dem sftp-Server eingerichtet.

Konfiguration Putty

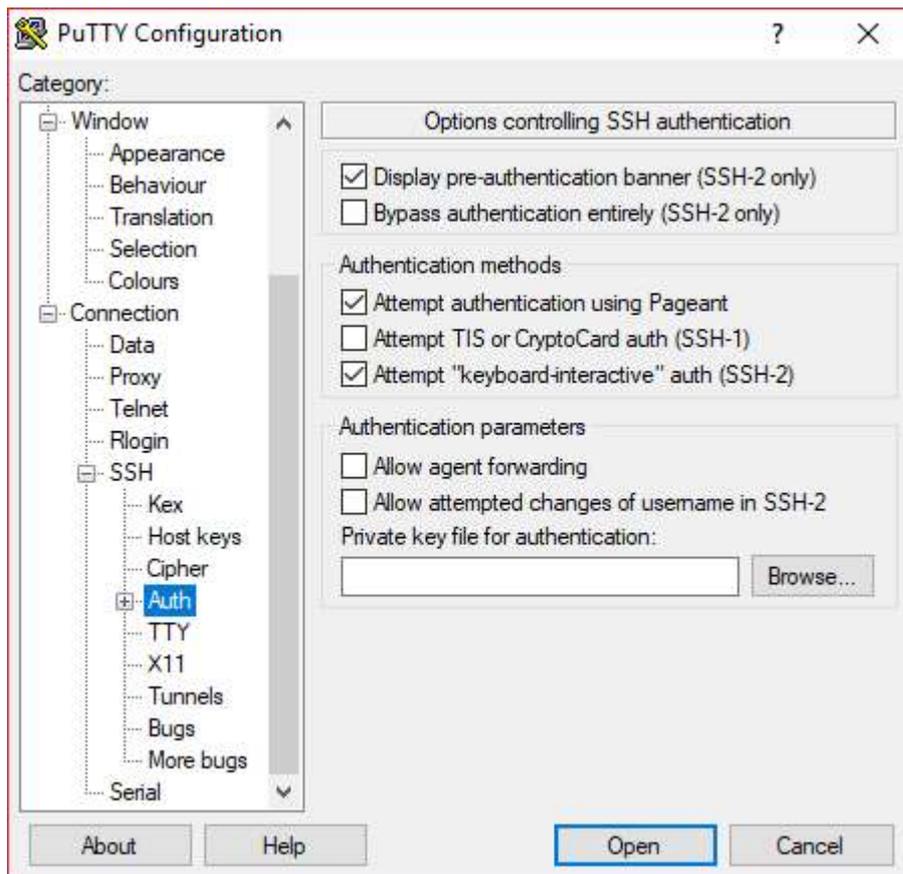
Jetzt muss Putty noch für die Benutzung der Keys konfiguriert werden. Putty starten und die vorher gespeicherte Session Laden (Load).



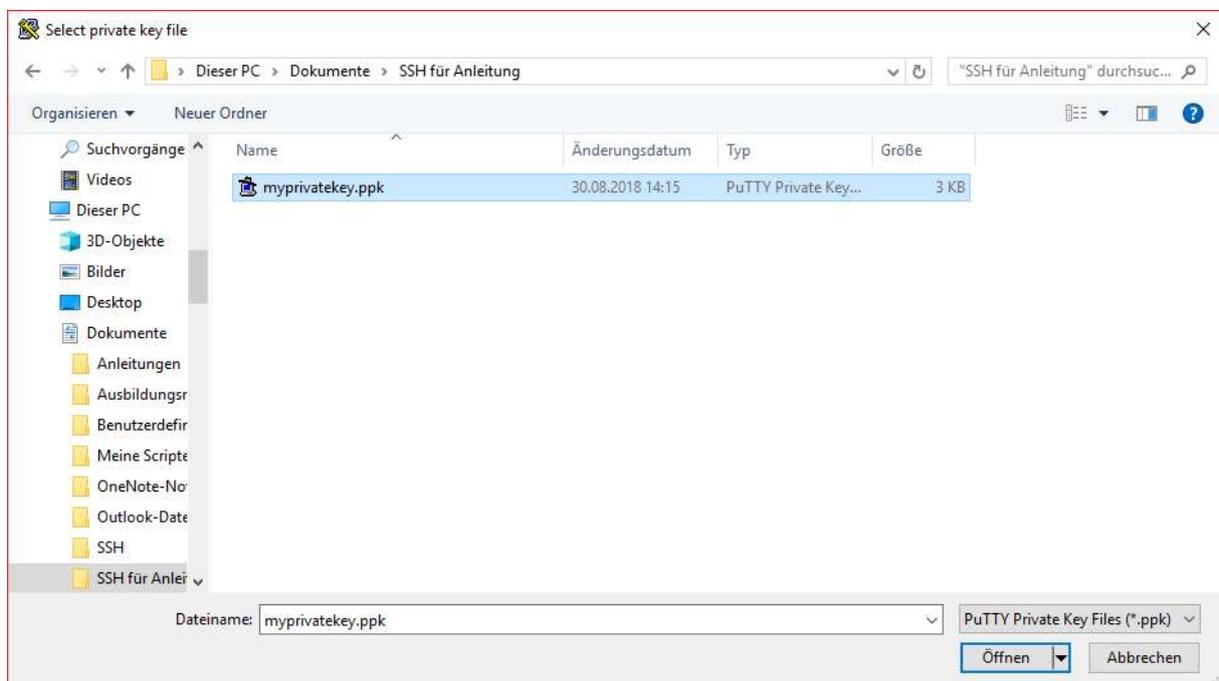
Unter Category, „Connection“ + „SSH“ auswählen (linke Seite).



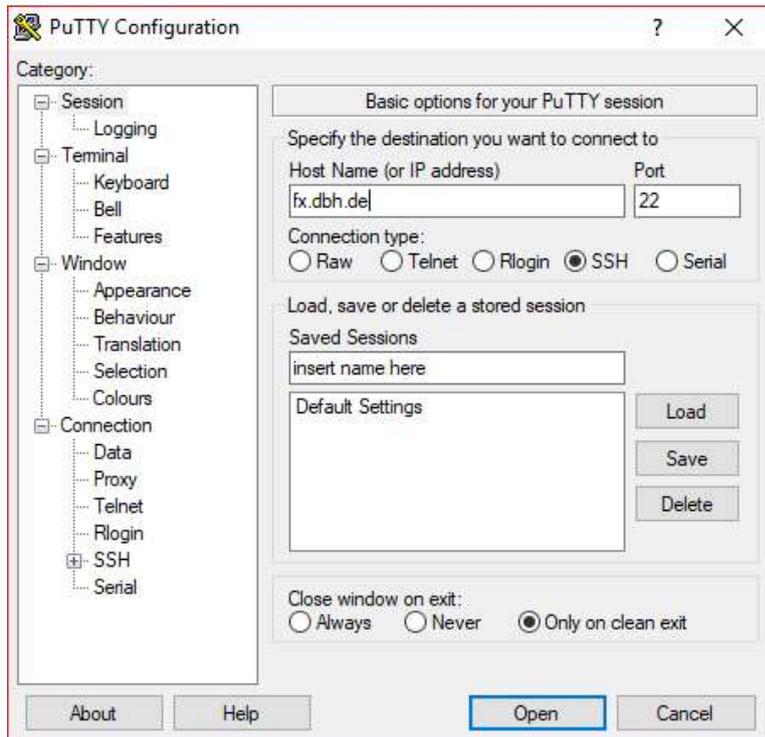
Unter „protocol options“ als „SSH protocol version:“ „2“ auswählen. Unter Category, „Connection“ + „SSH“ > „Auth“ auswählen.



Die zuvor erzeugte Datei des Private Keys unter "Authentication parameters" mit "Browse" auswählen und öffnen.



Die Session muss jetzt erneut gespeichert werden.



Dazu in der Category „Session“ „Save“ anklicken. Die so gespeicherte Session kann von psftp mit der „load“ Option verwendet werden.

Die Dokumentation zu Putty ist unter <https://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html> zu finden.