

DOCUMENTATION

Secure connection to the dbh Fileserver



Version 1.3

© 25.11.2019 dbh Logistics IT AG

Passing the manual on to third parties is strictly prohibited.

dbh Logistics IT AG

Martinistr. 47-49

28195 Bremen

IT Services ■ Customer Support

Contact person for inquiries: Customer Support

Service time: Mo. - Fr. 8:00 AM - 6:00PM

Tel. +49 421 30902-22

support@dbh.de

VERSION OVERVIEW

Date	Version	Changes	Author
09.10.2018	1.0	Correction of outdated information and pictures. translation (first draft)	NPo
10.10.2018	1.1	Small complements performed	SSc
11.10.2018	1.2	Contact person and phone number adjusted	NPo
25.11.2019	1.3	Point 6 is outdated and has been removed	NIh

Which Content has changed from the previous version?

Which Content is new in the current version?

The dbh fileserver exchanges import files of dbh applications, which are hosted in the datacenter of dbh Logistics IT AG. Dbh applications are running in a separate network segment. Connections via. Internet (for the data file exchange as well as webserver) stand in the demilitarized zone (dmz).

At first, we have to insure a secure connection between the affiliated clients to protect file transfers against other information flows on the Internet. The file transfer to the dbh through a sftp authentication with a public-key.

The following documentation describes 'how to set up a secure connection'.

CONTENT

1	Introduction	1
2	What is necessary?.....	1
2.1	Username/Password.....	1
2.2	Public Key	1
3	Installation/Configuration	2
4	Usage.....	2
4.1	Data transfer with OpenSSH with UNIX.....	2
	Public Key	2
	Batch operation.....	2
	Access.....	2
4.2	File Transfer with Putty	2
	Public Key	3
	Batch operation.....	3
	Access.....	3
5	Directories.....	4
6	Firewall Settings.....	4
7	Attachement.....	4
7.1	Attachment A: OpenSSH with UNIX/LINUX.....	4
	Public Key	4
7.2	Attachment C: Putty with Windows.....	5
	Public Key	6

8	Safety Note!.....	9
	Configuration of Putty	9

1 Introduction

SSH is a protocol suite, which provides an encoding for network services like 'remote login'(to connect to another computer and transfer data from one computer to the other).

Features:

- strong encryption
- X11 Forwarding (encrypts X Window System network traffic)
- Port Forwarding (encrypts certain channels for specific Protocols)
- strong authentication (Public Key, single-password and Kerberos authentication)
- interoperability (works with SSH 1.3, 1.5 and 2.0 protocol standards)
- data compression

2 What is necessary?

SSH client (SSH Version 2) for UNIX or Windows with file transfer Support (SFTP)

Free solution

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

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

-WinSCP (<https://winscp.net/eng/index.php>) for graphical interface

2.1 Username/Password

Authentication is done by entering the username and the password.

2.2 Public Key

The authentication is done through a pair of keys (public/private key). The Public Key is deposited on the file transfer server. This allows us a sign in without entering the password. If automated batch processes come into play, this is compulsorily needed. The configuration of the public key is basically the same on all platforms.

- generating the public/private keys
- transmission of the public keys onto the fileserver.

3 Installation/Configuration

Every product is described in the following attachments:

- OpenSSH with UNIX/LINUX (Attachment A)
- Putty (Attachment C)

4 Usage

4.1 Data transfer with OpenSSH with UNIX

Public Key

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

Files will be transmitted without entering a password.

Batch operation

The batch operation can be realized with a command file. The commands will be worked off systematically from top to bottom:

e.g. >batch.txt put *.xml
 >quit

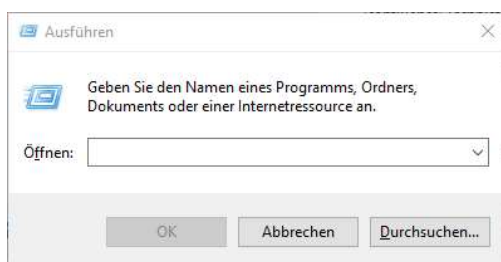
Transmits all xml files from the local directory to the home directory of the remote system.

Access

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

4.2 File Transfer with Putty

With 'right click on start -> execute' (key combination 'win' + 'R') starts an input window. This is where you have to search for 'psftp'. The file transfer to the file server is accomplished through the application 'psftp'.



Public Key

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

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

Files are transmitted without entering a password.

Batch operation

The batch operation can be realized with a command file. The commands will be worked off systematically from top to bottom:

e.g. >batch.txt put *.xml
 >quit

Transmits all xml files from the local directory to the home directory of the remote system.

Access

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

Every sftp command can be realized inside a command file.

```
C:\Programme\Putty>psftp
psftp: no hostname specified; use "open host.name" to connect
psftp> help
! run a local command by 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
machine 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 Directories

Every user has two folders (import and export) according to the standard on the file server for file transfers. Files, which are transferred onto the dbh file server, have to be saved into the folder 'import'. Files for the customer will be provided in the folder 'export'. After a successful Transmission, every file has to be deleted or saved in a subdirectory.

6 Firewall Settings

Port 22 has to be approved in order to allow a sftp communication starting from the 'fx.dbh.de'. (194.99.88.17)

7 Attachement

7.1 Attachment A: OpenSSH with UNIX/LINUX

Installation of OpenSSH with instructions.

Public Key

To generate the public and private key pair you have to enter 'ssh-keygen'.

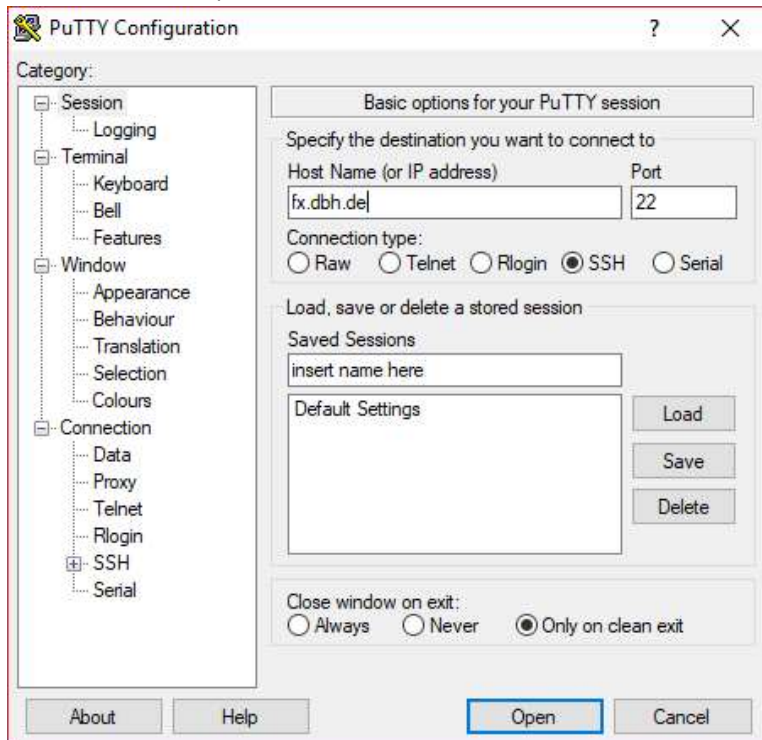
```
$ ssh-keygen -t rsa -b 2048 <RETURN>
$ Generating public/private dsa key pair.
$ Enter file in which to save the key (/homedir/.ssh/id_rsa):<RETURN>
Enter passphrase (empty for no passphrase):<RETURN>
Enter same passphrase again: <RETURN>
Your identification has been saved in /homedir/.ssh/id_rsa.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

After the terminal requests you to enter a passphrase, you SHOULD NOT enter anything. Instead, you just press <RETURN> twice to finish the configuration. There should be a file called 'id_rsa.pub' inside the directory '/homedir/.ssh/'.

This file will be transmitted in to the mail account of <mailto:support@dbh.de> and installed on the sftp server

7.2 Attachment C: Putty with Windows

Download of the installer package on the following website: <https://the.earth.li/~sgtatham/putty/0.70/w32/>. This is where you are able to download the newest version (putty-'version'-installer.msi). The installation starts with a simple double click. You should be able to start putty after a successful installation.

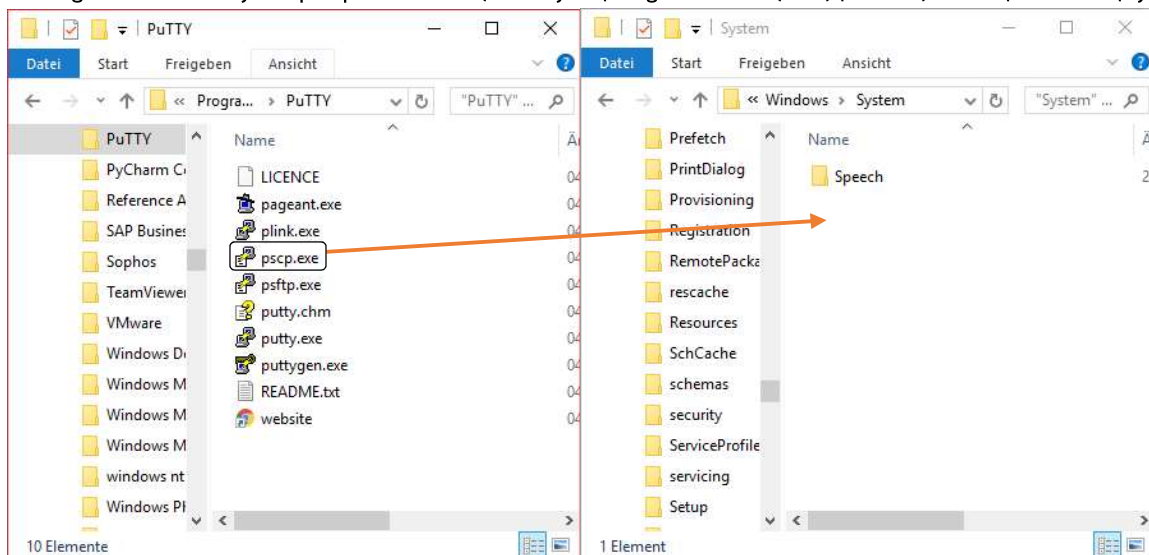


-Insert the server name (fx.dbh.de) into the input box 'Host Name (or IP address)'.

-'Connection type' = SSH

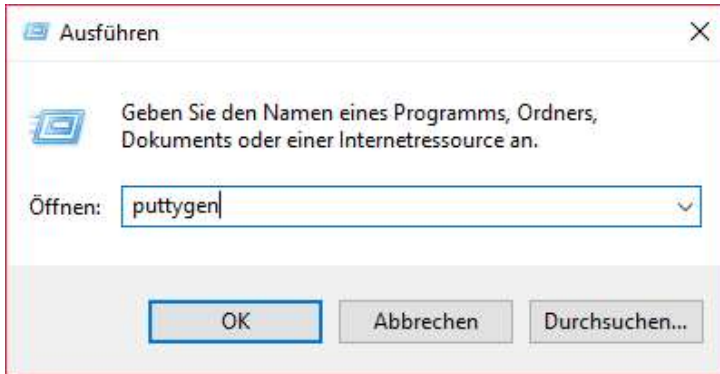
-Insert a name of your choice into the input box 'Saved sessions'. Use 'Save' to save your session.

-Change the directory of 'psftp.exe' from (usually 'C:\Program Files (x86)\PuTTY') to 'C:\Windows\System'.

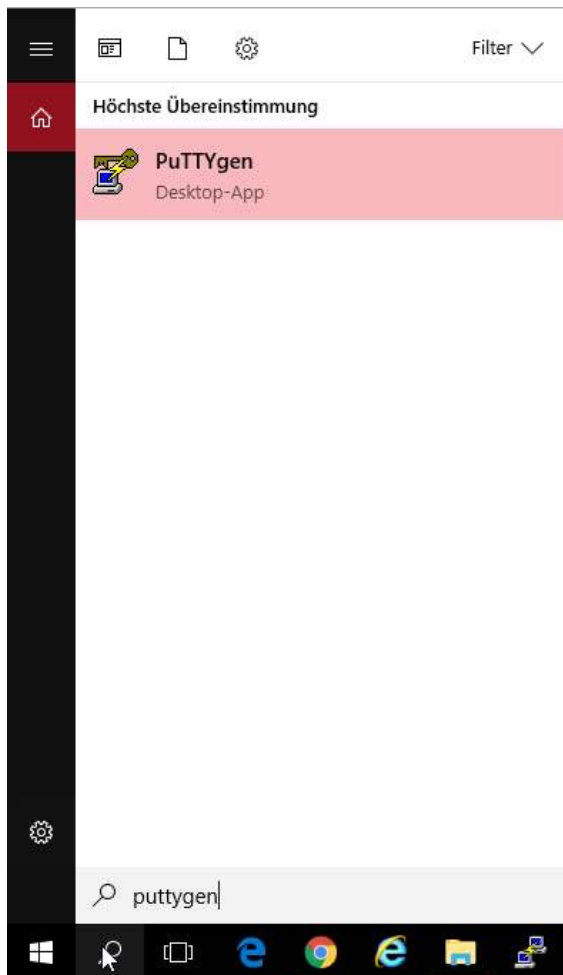


Public Key

After the installation is finished successfully, the first thing to do is generating the key pair.

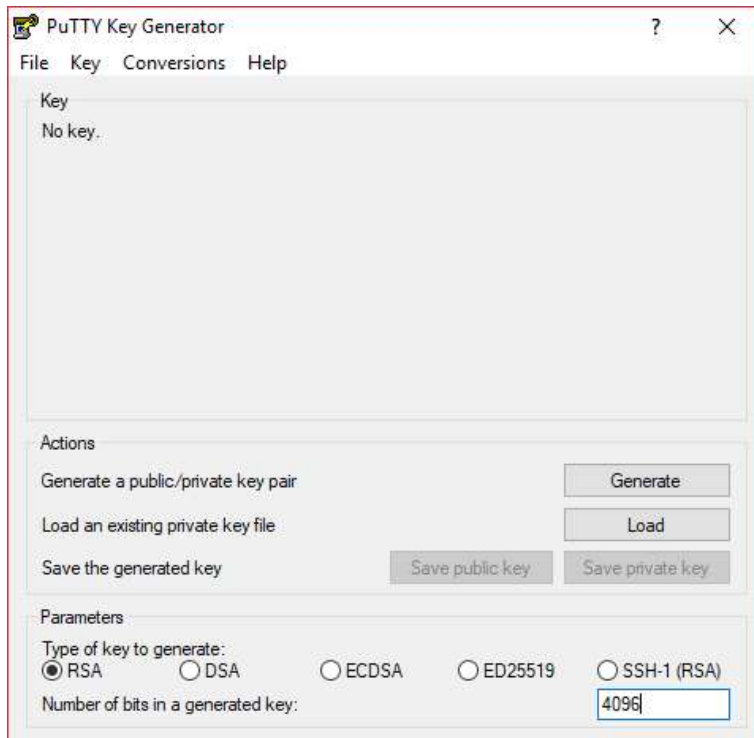


With 'right click on start -> execute' (key combination 'win' + 'R') starts an input window. This is where you have to search for 'puttygen'.

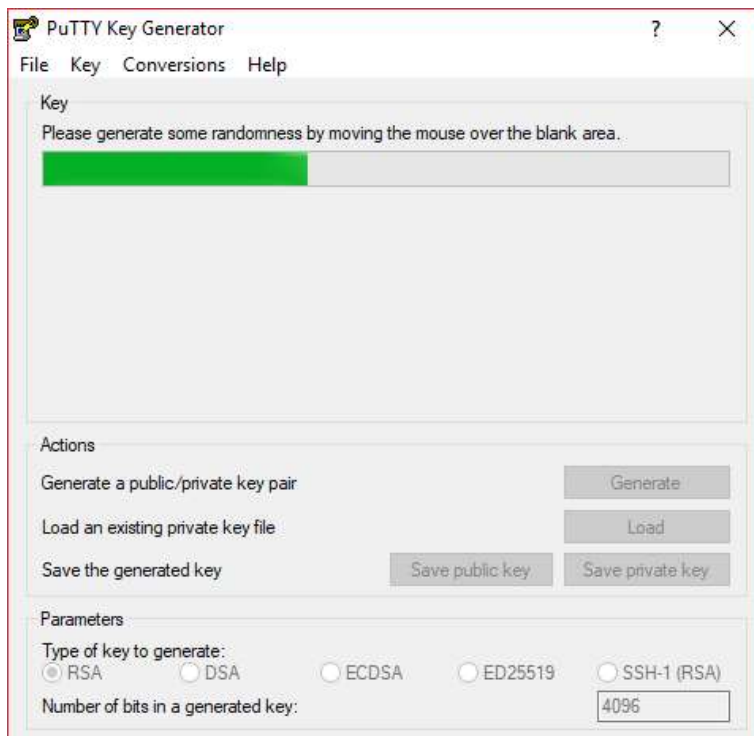


Otherwise, use the Windows search bar to search for 'puttygen'.

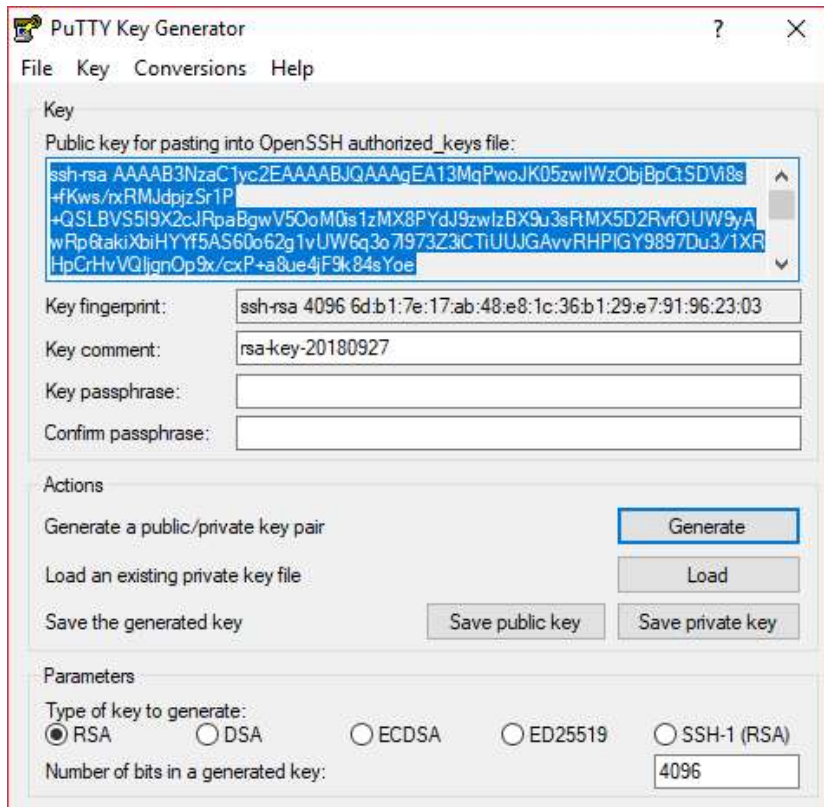
Under 'Type of key to generate' tick of the box which says 'RSA' and change the Number of bits in a generated key to 4096.



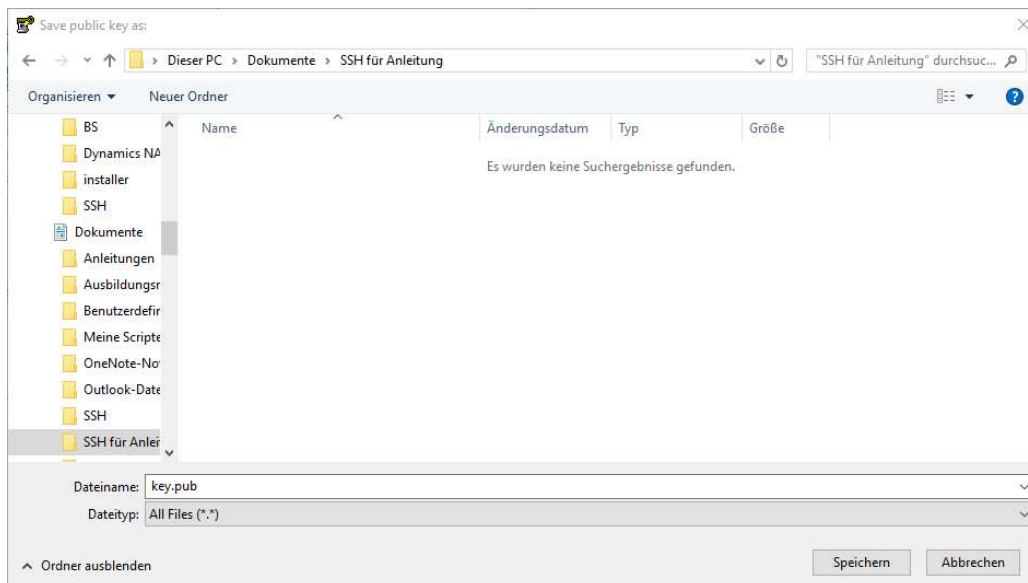
Start the process by pressing 'Generate'. Once an empty progress bar appears, randomly move the mouse over the empty window space until the progress bar is full to generate the key.



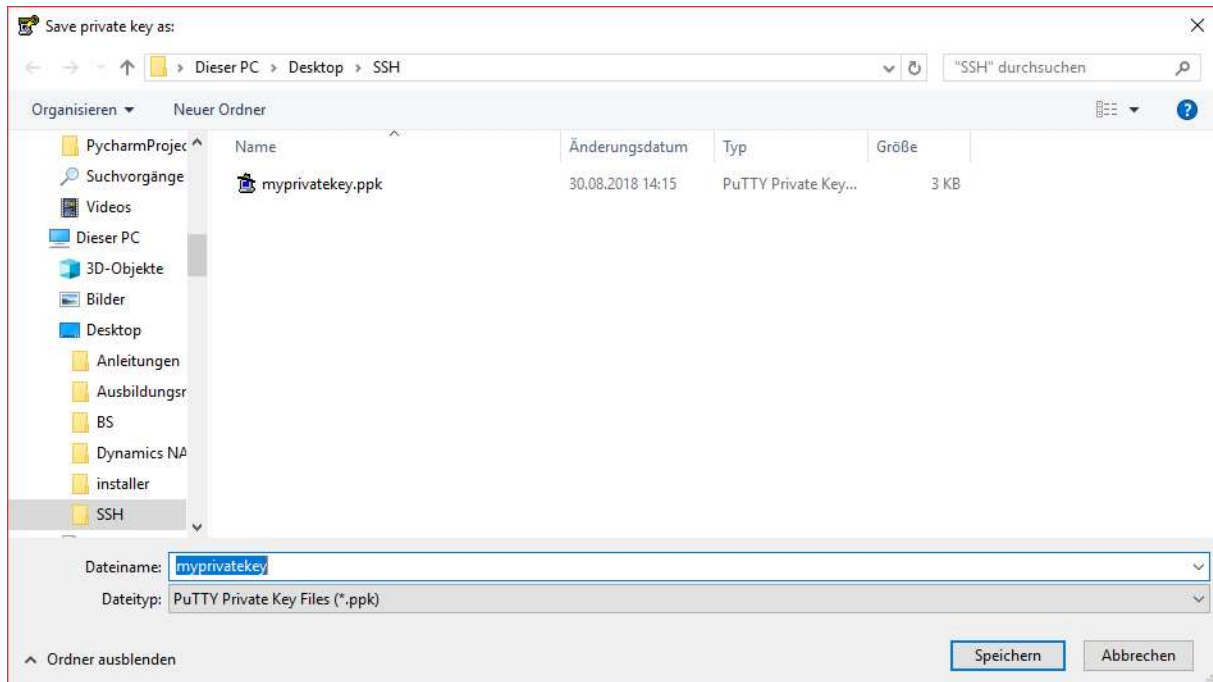
Generating the key pair might take a couple of minutes.



Save the public key by pressing 'Save public key'.



Afterwards you need to press 'Save private key' to save your piece of the key pair. The warning has to be answered with 'yes'.



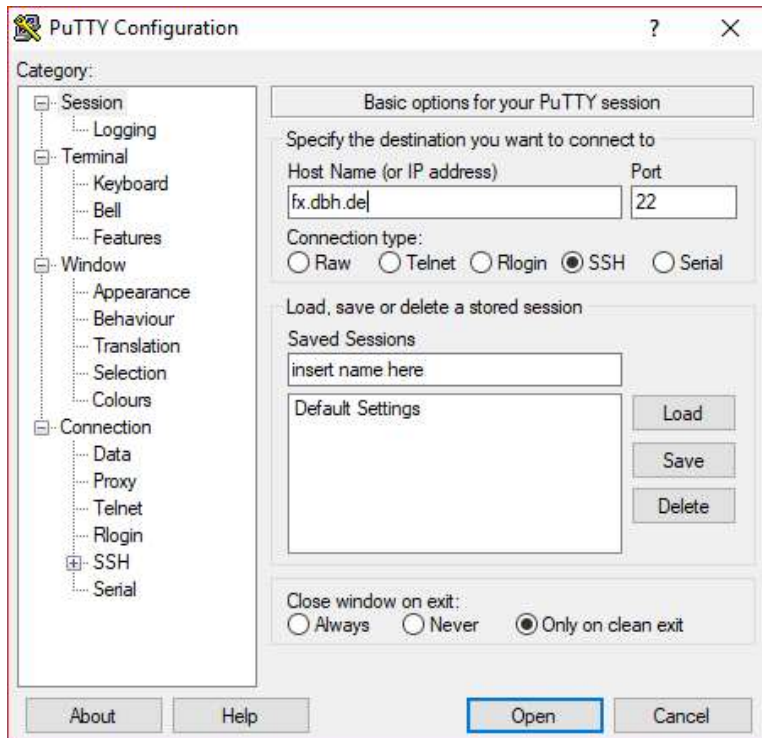
8 Safety Note!

Saving the private keys without a passphrase provides a potential security risk. You should take appropriate measurements to insure that only entitled people have access to the private key.

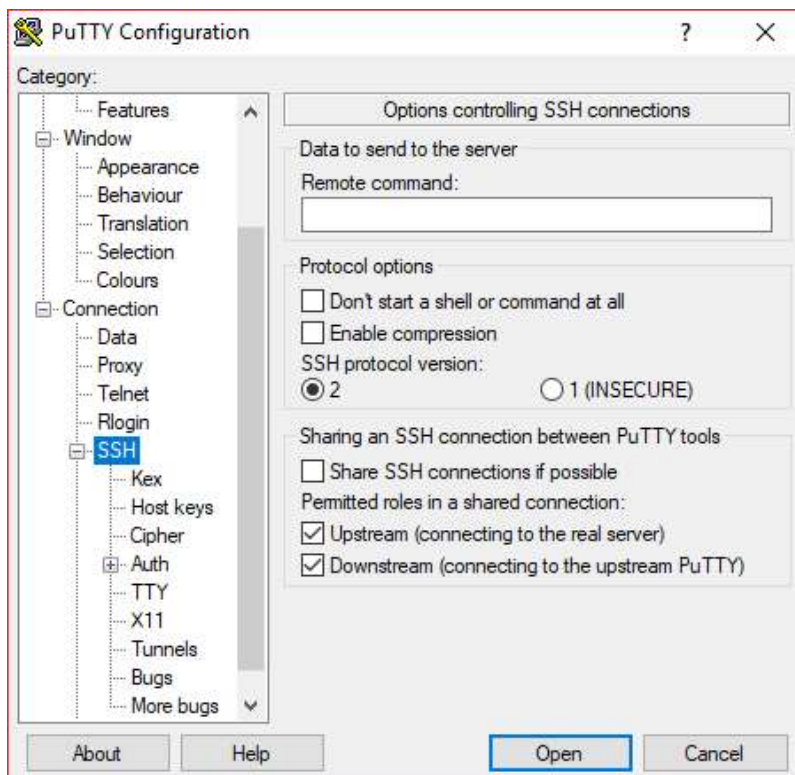
The File with the public key (key.pub) has to be send to the following email: 'support@dbh.de' and will be deposited on the sftp-server.

Configuration of Putty

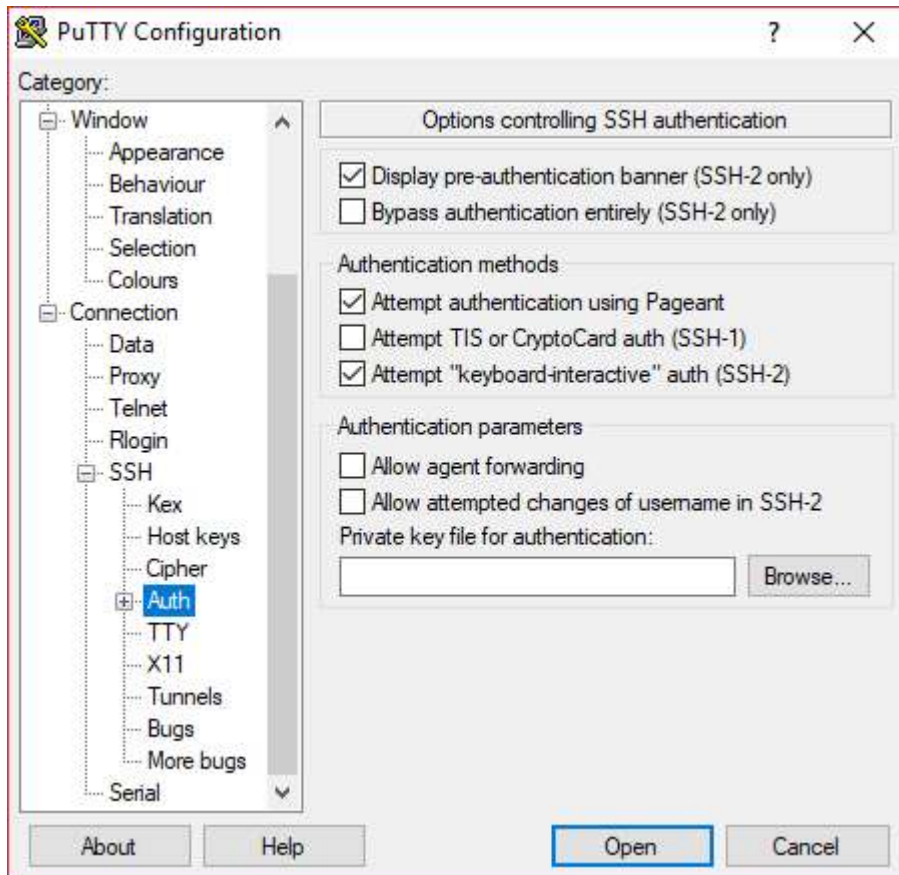
Putty has to be set up in order to use keys. Therefore, start putty and open the previously saved session.



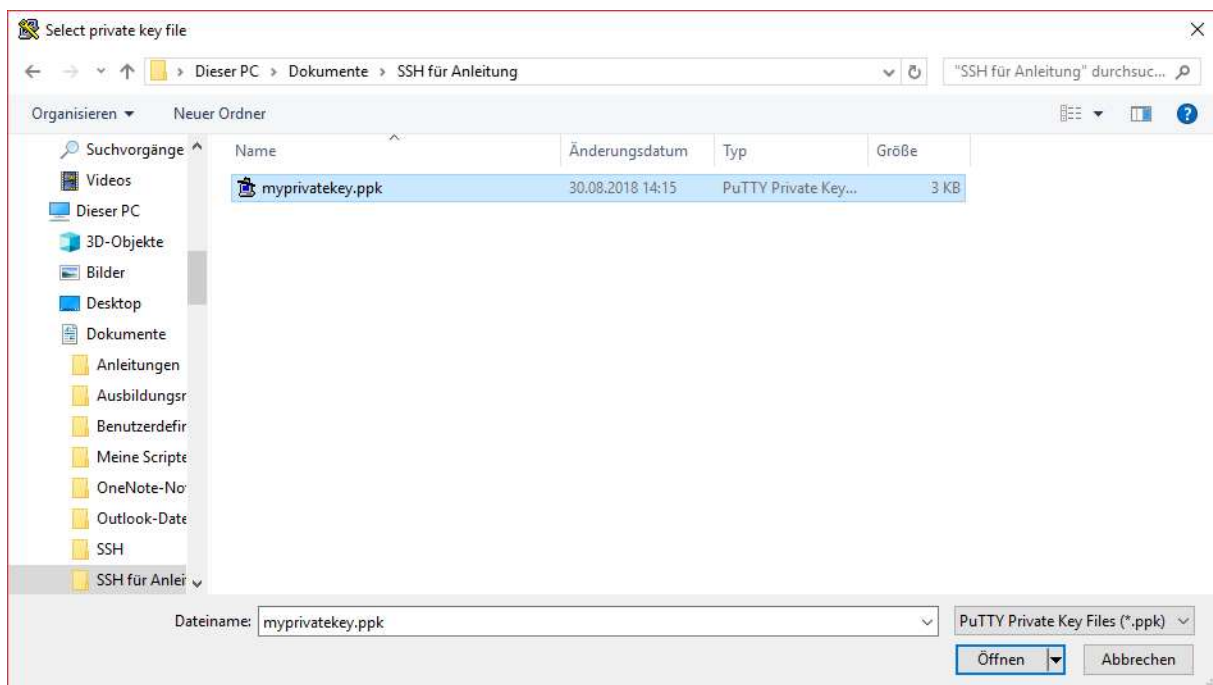
Under 'Category' select 'SSH' (left side).



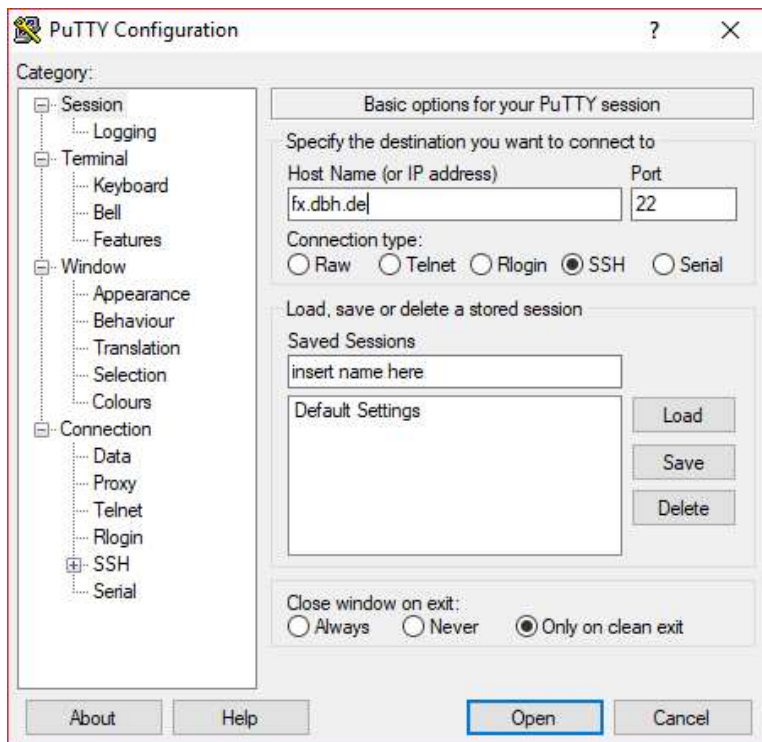
Under 'SSH protocol version' tick of the box that says '2'. Then select under 'SSH' > 'Auth'.



Open the previously generated file of the private key in the input box 'Private key file for authentication' with the function 'Browse'.



You have to save your session now again.



Therefore, press 'session' (left side) and 'Save'. This saved session will be re-opened from psftp with the command 'load'.

The documentation of putty can be read on the following webpage: '<https://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html>'.