How to Public key authentication with freeSSHd

Enthaltene Funktionen

- Umstellung auf Public key authentication
- Generierung eines Private keys mit PuTTY Key Generator
- Verbindung testen

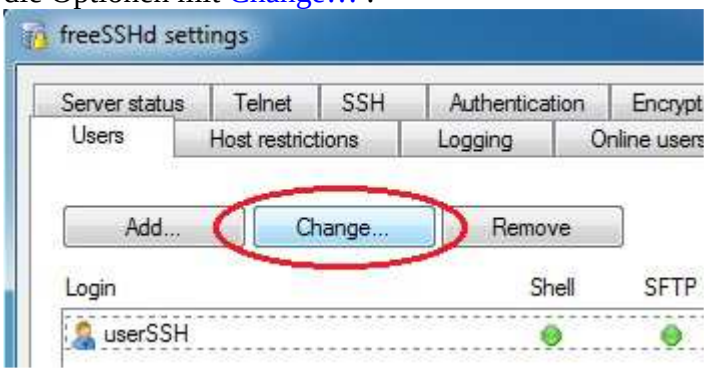
Voraussetzung

Dieses Tutorial basiert auf einer bereits vorhandenen Installation von freeSSHd und setzt diese voraus. Sollten Sie freeSSHd noch nicht installiert haben, so können Sie folgendes Tutorial verwenden:
http://johann-scharl.de/instructions/How to install freeSSHd.pdf

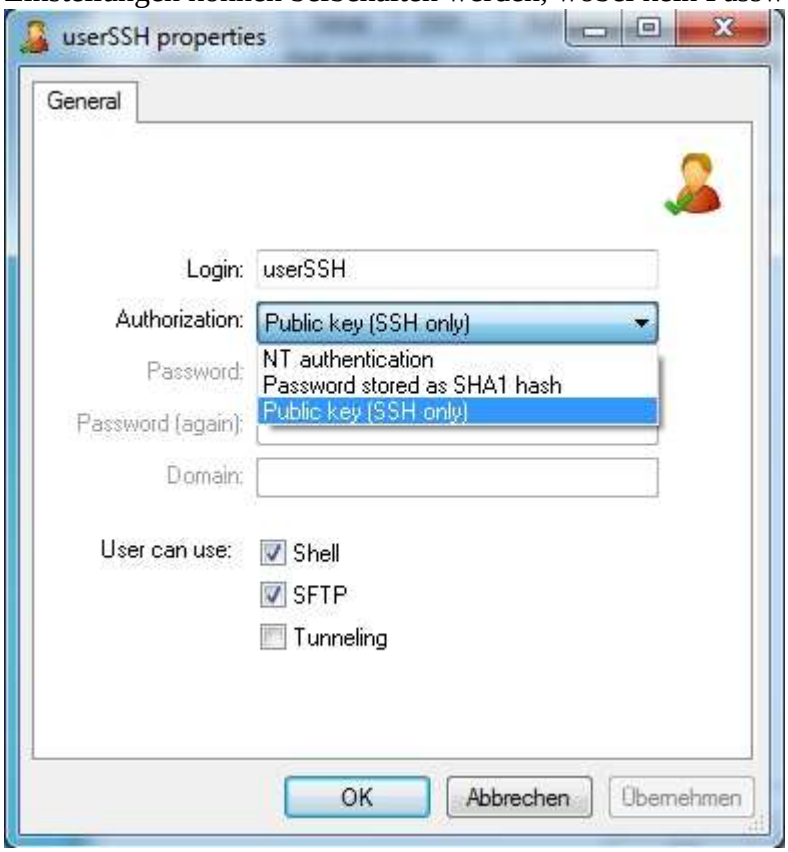
1. Umstellung auf Public key authentication Funktionalität

- Damit eine gesicherte Verbindung mit einem Privaten Schlüssel erfolgen kann, muss freeSSHd entspr. konfiguriert werden. Als erstes öffnen Sie die Programmoberfläche von freeSSHd am Server:

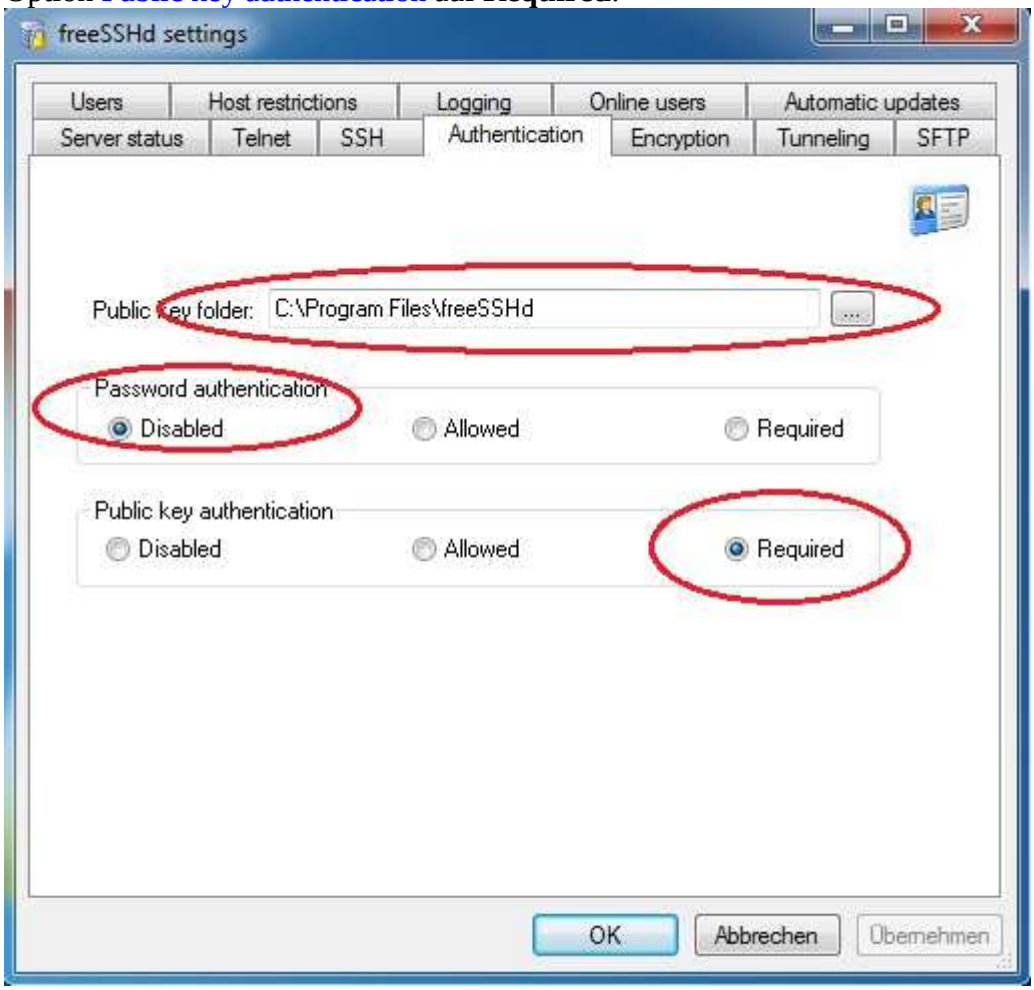
Klicken Sie dann auf den Reiter <Users>, markieren Sie den angelegten Benutzer und öffnen Sie die Optionen mit Change… :



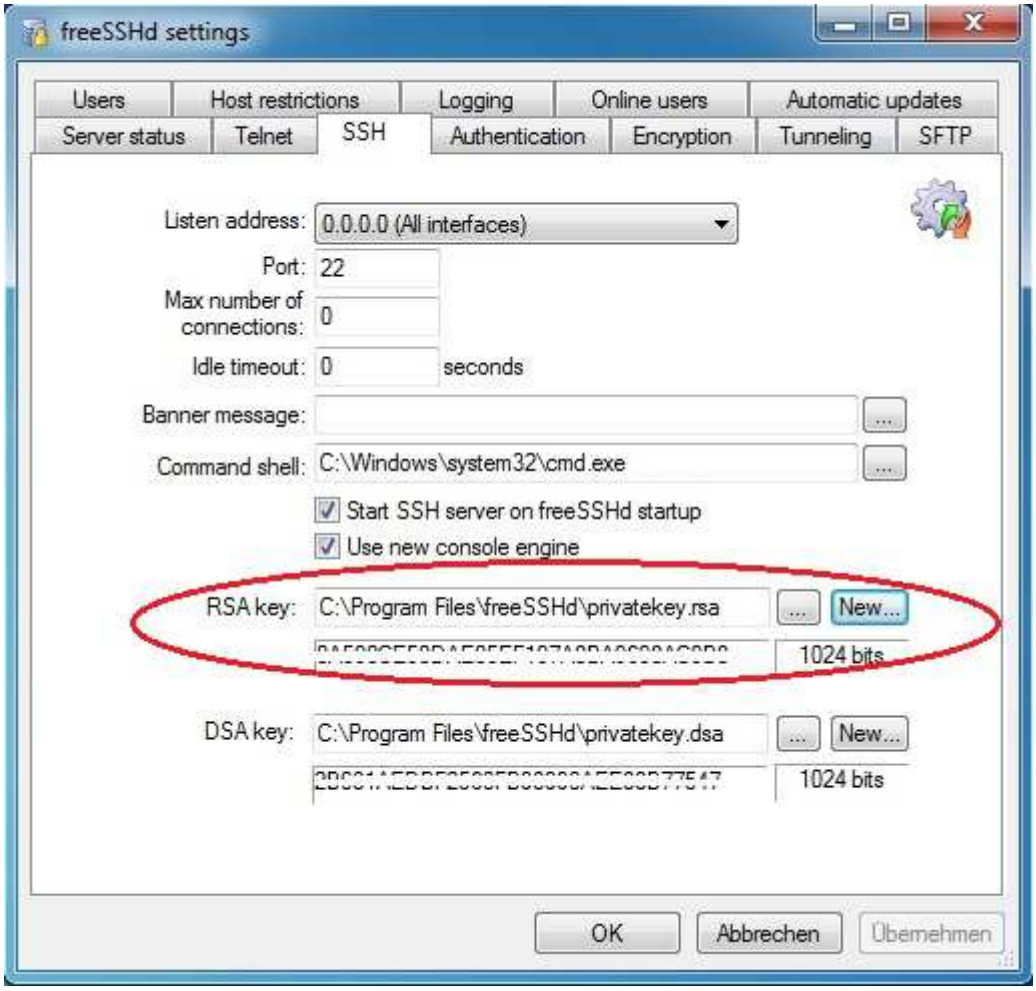
Verwenden Sie für die Option Authorization: **Public key (SSH only)**, die restlichen Einstellungen können beibehalten werden, wobei kein Passwort vergeben werden kann:



Klicken Sie auf OK um die Einstellungen zu verlassen. Wechseln Sie zum Reiter <Authentication> und stellen Sie die Option Password authentication auf **Disabled** und die Option Public key authentication auf **Required**:



Die Einstellung für Public key folder können wir so belassen. Diese ist Standard: C:\Program Files\freeSSHd
Nun wechseln Sie zum Reiter <SSH> und prüfen, ob der RSA key vorhanden ist, wenn nicht, müssen Sie einen neuen erstellen mit: New → 1024 bits

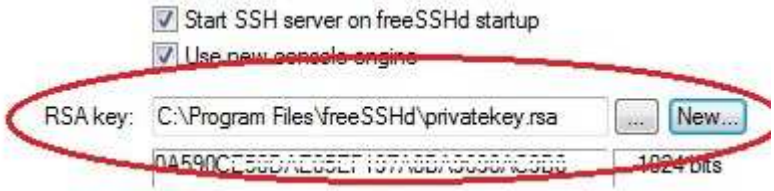


Übernehmen und beenden Sie die Einstellungen mit **OK**.
Die Umstellung ist somit abgeschlossen und damit diese Einstellungen auch verwendet werden, muss der Dienst neu gestartet werden (**WICHTIG!**):

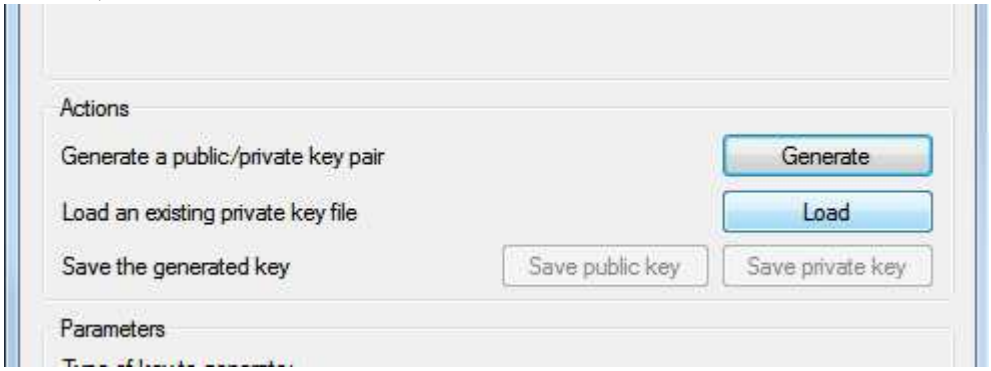
2. Generierung eines Privaten Schlüssels mit PuTTY key Generator

- Die Umstellung für die Funktionalität mit Public key authentication ist nun kpl. und setzt nun einen öffentlichen und privaten Schlüssel für die Verbindung voraus. Ein öffentlicher Schlüssel muss nun aus den Informationen des privaten Schlüssels erzeugt werden.

Der private Schlüssel ist bereits im Programmverzeichnis von freeSSHd abgelegt:



Genau aus dieser Datei **privatekey.rsa** muss nun das Schlüsselpaar generiert werden.
Hierfür benutzen wir das Tool: **puttygen.exe**
Dieses können Sie direkt unter folgendem Link downloaden:
http://johann-scharl.de/tools/puttygen.exe
Nachdem Sie puttygen.exe gestartet haben muss als erstes der Private Schlüssel geladen werden, hierfür klicken Sie auf **Load**:

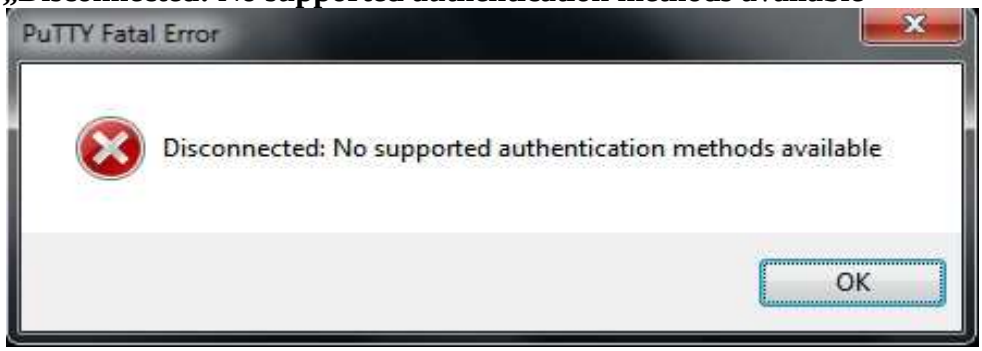


Wählen Sie dann die Datei **privatekey.rsa** aus und bestätigen die Eingabe mit **Öffnen**:
(Info: Damit die Dateiendung .rsa ausgewählt werden kann, müssen Sie den Dateityp auf **All Files (*.*)** umstellen)

puttygen teilt Ihnen dann mit, dass der Schlüssel ein Fremdschlüssel ist und für die Verwendung mit PuTTY ein eigenes Format benötigt wird:

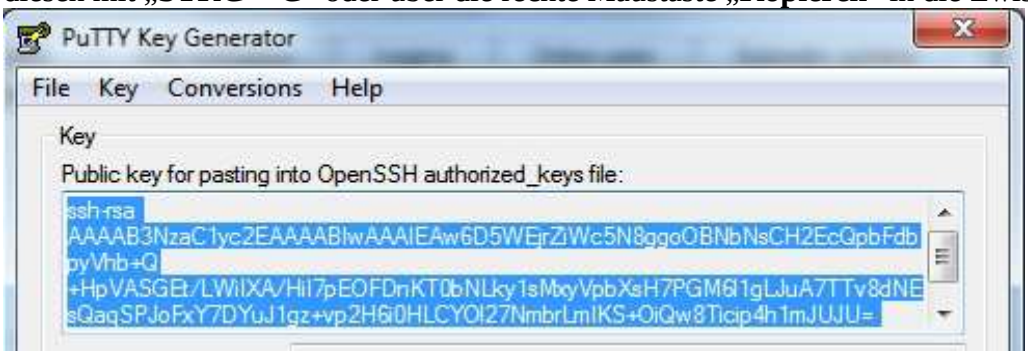
Bestätigen Sie diese Meldung mit **OK**.

WICHTIG! Die folgenden Schritte sind wichtig und müssen genau so wie beschrieben eingehalten werden! Bei Nichtbeachtung kommt es immer wieder vor, dass eine Anmeldung abgewiesen wird, mit folgender Meldung:
„Disconnected: No supported authentication methods available“

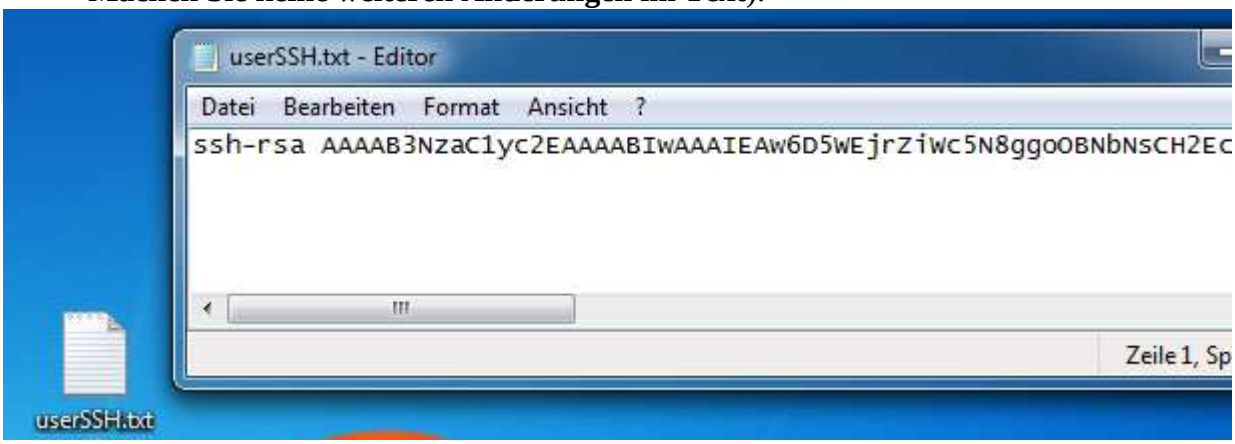


Diese Fehlermeldung deutet darauf hin, dass ein inkorrekter Schlüssel verwendet wurde. freeSSHd protokolliert dies auch im error-log:
„SSH userSSH disconnected.“

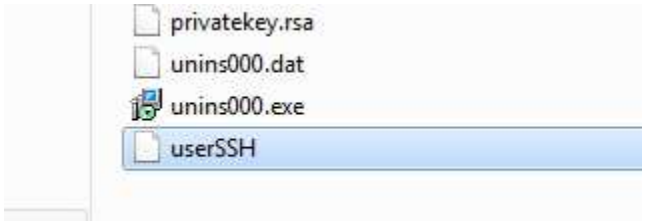
Markieren Sie den kpl. key im Fenster **(Achtung! Scrollen nicht vergessen!**) und kopieren Sie diesen mit „**STRG + C**“ oder über die rechte Maustaste „**Kopieren**“ in die Zwischenablage:



Erstellen Sie dann ein leeres Textdokument z.B. auf dem Desktop oder gleich direkt in das Verzeichnis von freeSSHd (**C:\Program Files\freeSSHd**). Der Name dieser Textdatei sollte wenn möglich dem Benutzernamen für den Login gleichen, hier also **userSSH.txt**. Öffnen Sie jetzt diese Datei, fügen Sie den kopierten Text ein und speichern die Textdatei (**WICHTIG! Machen Sie keine weiteren Änderungen im Text**):

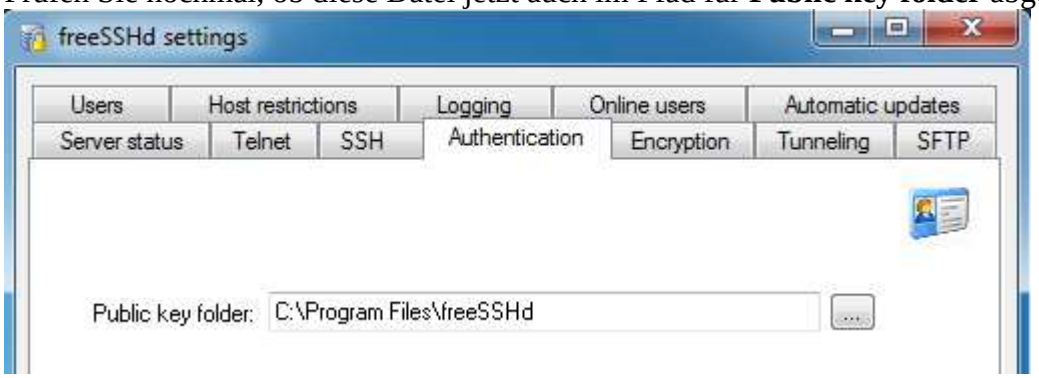


Nun muss diese Datei **userSSH.txt** umbenannt werden in **userSSH** also **ohne** Dateierweiterung:

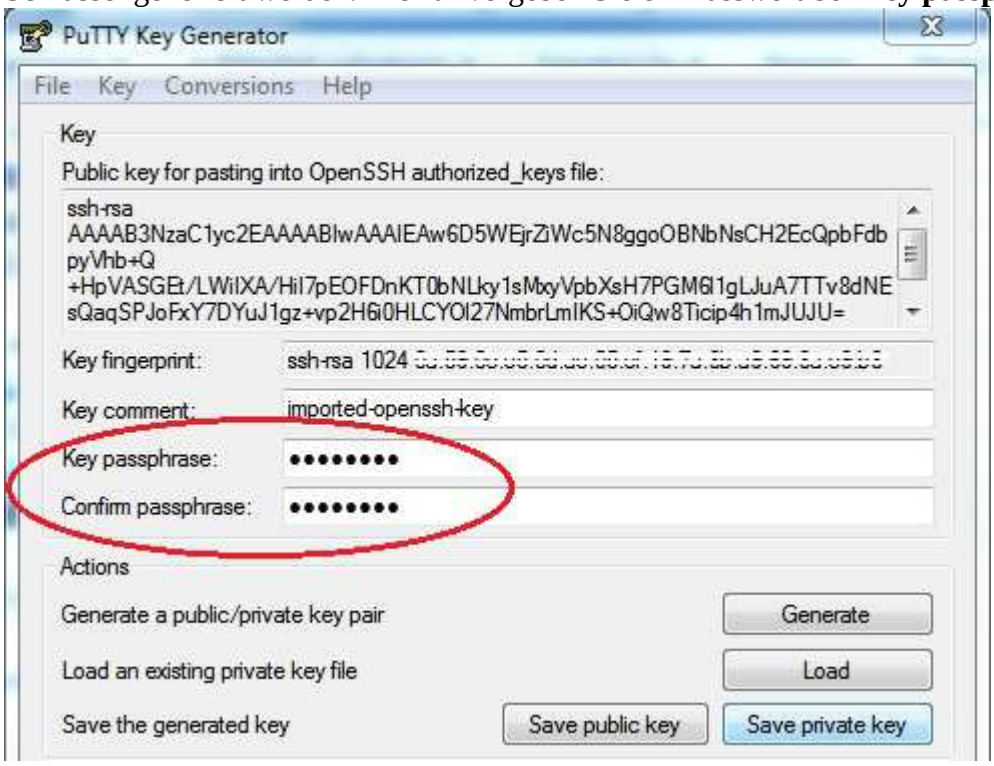


WICHTIG! Das Umbenennen der Datei muss DRINGEND erst NACH dem Speichern erfolgen! Eine andere Vorgehensweise führte immer zur o.g. Fehlermeldung bei einem Anmeldeversuch mit PuTTY.

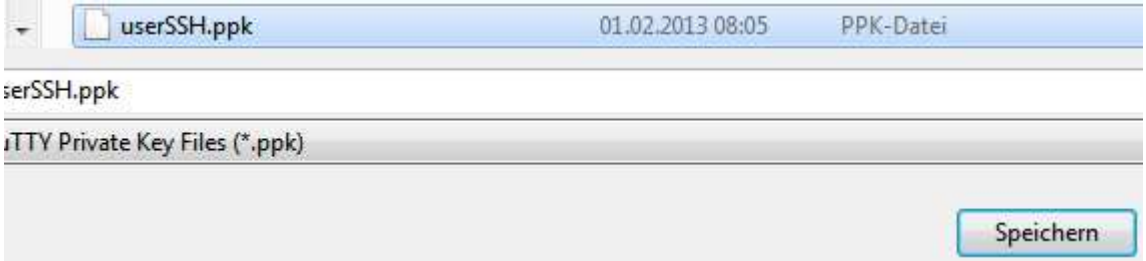
Prüfen Sie nochmal, ob diese Datei jetzt auch im Pfad für **Public key folder** abgelegt ist:



Nachdem der öffentliche Schlüssel gespeichert wurde, muss nun der dazugehörige Private Schlüssel generiert werden. Hierfür vergeben Sie ein Passwort bei **Key passphrase + Confirm**:



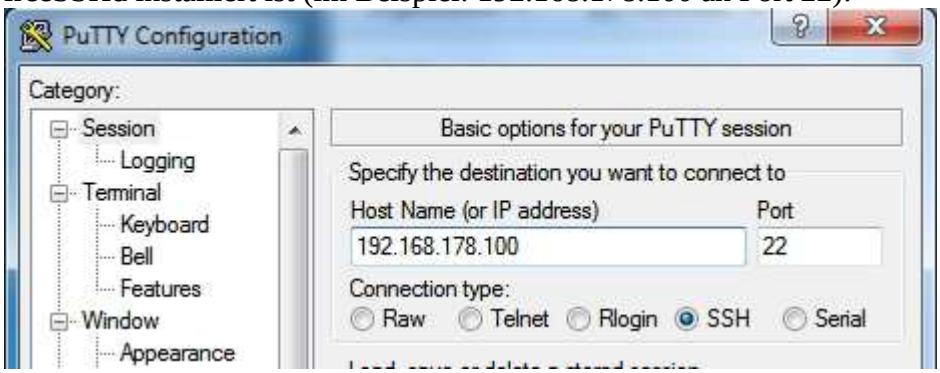
Das Passwort müssen Sie Sich gut merken! Eine Verbindung mit falschen Passwort nicht möglich. Speichern Sie nun den Privaten Schlüssel mit **Save private key** an einen gewünschten Ort, wobei als Name der gleiche des öffentlichen Schlüssels verwendet werden sollte:



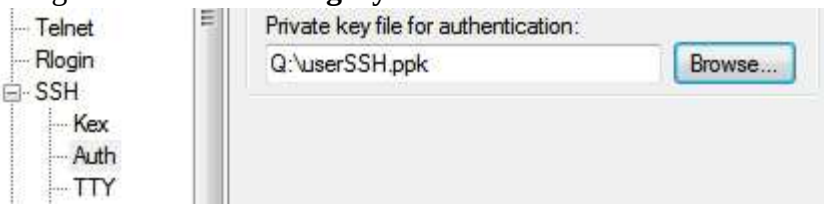
Die Dateierweiterung ist hier **.ppk** und sollte auch beibehalten werden. Diesen Schlüssel benötigen wir dann später für PuTTY. Nachdem wir nun beide Schlüssel generiert haben können wir das Tool puttygen schließen.

3. Verbindung herstellen mit PuTTY

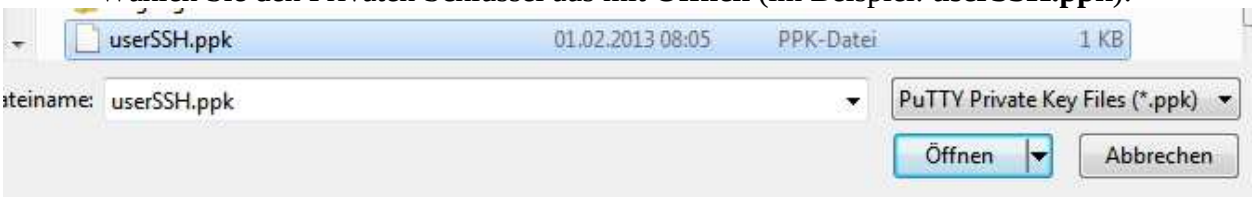
- Um eine Verbindung mit PuTTY herzustellen, starten Sie PuTTY auf einen anderen Rechner und geben als Host-Name die IP-Adresse oder den Rechnernamen des Servers an, auf welchem freeSSHd installiert ist (im Beispiel: 192.168.178.100 an Port 22):



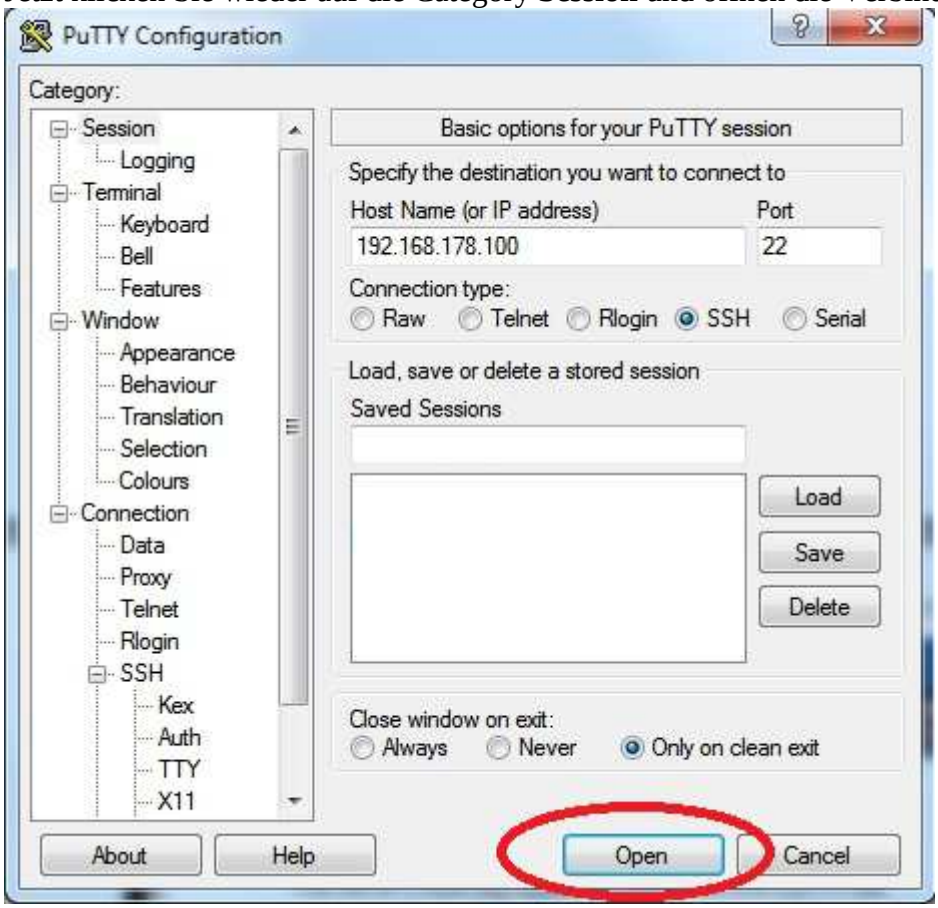
Bevor wir die Verbindung nun öffnen können, muss der Private Schlüssel ausgewählt werden! Navigieren Sie unter **Category SSH → Auth** und klicken Sie auf **Browse…**:



Wählen Sie den Privaten Schlüssel aus mit **Öffnen** (im Beispiel: **userSSH.ppk**):



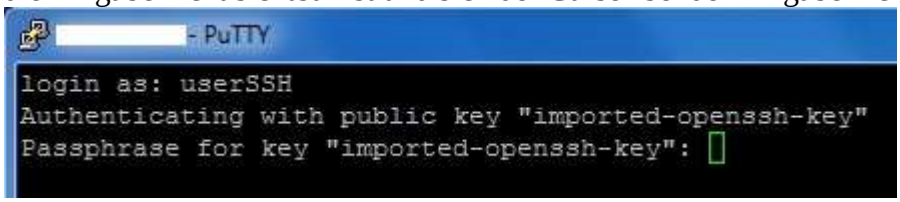
Jetzt klicken Sie wieder auf die Category **Session** und öffnen die Verbindung mit **Open**:



PuTTY sollte dann die erste Anmeldung mit folgendem Hinweis warnen:

Diese Meldung könne Sie mit Ja bestätigen, somit wird der Fingerprint der Schlüsseldatei eingetragen und muss bei der nächsten Verbindung nicht erneut bestätigt werden. Jetzt sollten Sie den Benutzernamen angeben können (im Beispiel: **userSSH**):

Bestätigen Sie die Eingabe mit {ENTER} und geben Sie nun das Passwort (Passphrase) für den Privaten Schlüssel an, welchen Sie in puttygen angegeben haben. Beachten Sie hier wieder, dass die Eingabe nicht sichtbar ist und sich der Cursor bei der Eingabe nicht bewegt:



Mit dem Hinweis: „Authenticating with public key“ werden Sie darauf hingewiesen, dass eine Anmeldung nur mit einem Privaten Schlüssel möglich ist. Nachdem Sie das Passwort bestätigt haben, wird die Verbindung hergestellt: