SSH Authentifizierung per Key-File mit PuTTY

Vorraussetzungen:

- OpenSSH Server
- PuTTY Client
- PuTTYgen

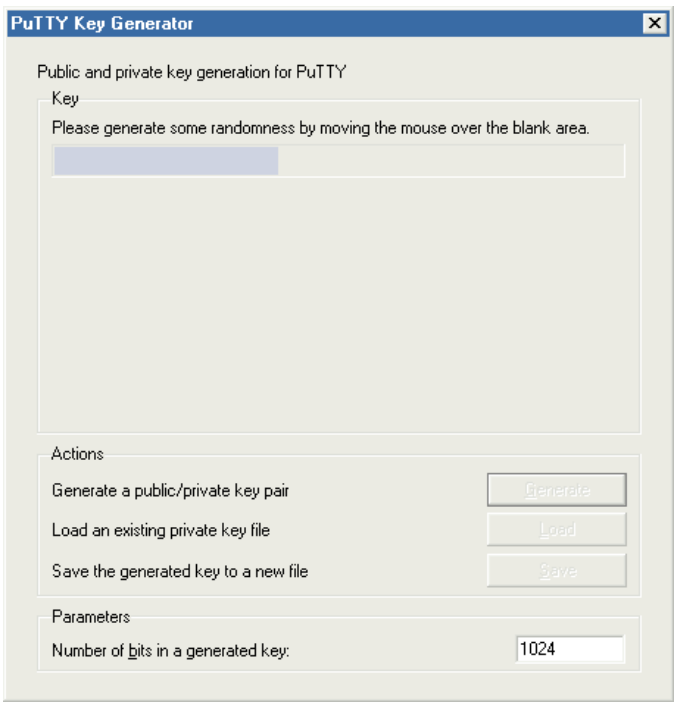
Um eine höhere Sicherheit bei der Anmeldung an einem Linux Server bereitstellen zu können ist es empfehlenswert auf die Methode der Authentifizierung per RSA Keys umzusteigen.

Wir gehen hier davon aus, das auf dem Server das OpenSSH Paket schon installiert ist und der Login für den User per Username und Passwort schon ohne Probleme über PuTTY funktioniert.

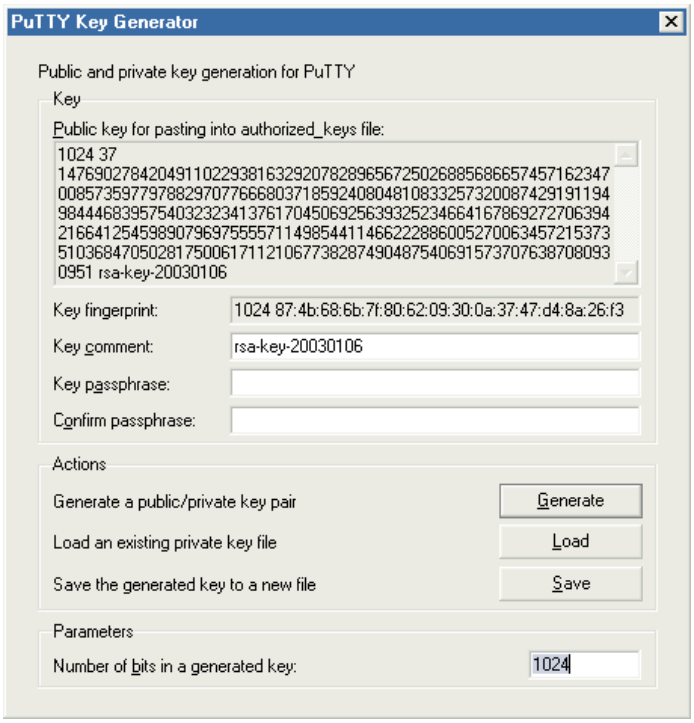
Was ist zu tun ?

Erst einmal brauchen wir das Tool PuTTYgen, um ein RSA Schlüssel zu generieren.
Download kann man PuTTYgen hier: http://www.putty.nl/latest/puttygen.exe

Nach dem Download startet man PuTTYgen und bewegt die Maus solange bis das Programm einen Public Key generiert hat.



Nachdem die Generierung fertiggestellt ist, hat man noch die Möglichkeit den „Key comment“ zu ändern und eine Passphrase anzugeben.
Es wäre auch möglich keine Passphrase anzugeben, **davon ist aber auf jeden Fall abzuraten.**



Dann speichert man das ganze noch über den „Save“ Button auf dem rechner ab.

ACHTUNG:
Dieses private Key File darf auf keinen Fall auf den Server geladen werden, bzw. einer anderen Person zugänglich gemacht werden. Ansonsten ist es dieser Person mit der richtigen Passphrase möglich sich auf dem Server einzuloggen, bzw. wenn sie erst gar keine Passphrase gesetzt haben, ist es möglich sich lediglich mit diesem private Key File auf dem Server einzuloggen.

Nun muss der Public Key der bei der Mausbewegung erzeugt wurde auf den Server kopiert werden. Also den oberen Teil wo im Feld
„Public key for pasting into authorized_keys file:“
per <STRG> + <C> in die Zwischenablage kopieren.

Jetzt müssen Sie sich per SSH wie gewohnt auf dem Server einloggen und in Ihr Userverzeichnis wechseln, wenn Sie da noch nicht sind.

Erstellen Sie dort falls noch nicht vorhanden den Ordner **.ssh** und darin die Datei **authorized_keys**. In diese Datei fügen Sie den Public Key Schlüssel wo sie vorher in die Zwischenablage kopiert haben ein.

Achtung:
es darf kein Zeilenumbruch eingefügt werden, d.h. der Key steht in einer einzigen Zeile und auch nach dem Key darf kein Zeilenumbruch eingefügt werden.

Dann speichern Sie die authorized_keys Datei ab.

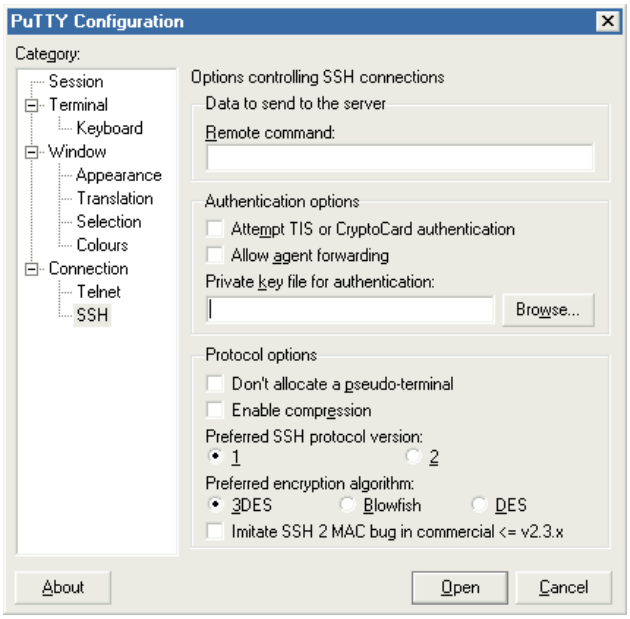
Nun müssen noch die Zugriffsberechtigungen gesetzt werden.

Dazu gehen Sie wieder in Ihr Homeverzeichnis und führen dort folgende befehle aus:

```
chmod 700 .ssh
chmod 400 .ssh/authorized_keys
```

Damit haben lediglich Sie die Berechtigung die Datei zu lessen !!!

Soweit war es das nun auch.
Lediglich muss in PuTTY nun noch das vorher abgespeicherte private Key File eingegeben werden.



Also unter „Private key file for authentication“ Ihr private Key File auswählen.

Nun können Sie Die Verbindung herstellen.
Das Login läuft dann so ab, das Sie den Usernamen eingeben und dann die Passphrase eingeben müssen, sofern Sie eine eingegeben haben.

Herzlichen Glückwunsch...
Sie haben es geschafft und das Login per Authetication Keys erfolgreich eingerichtet.

Wenn Sie sicher sind das der Login per Keys funktioniert können Sie aus Sicherheitsgründen den normalen Login deaktivieren.

Dazu ändern Sie folgenden Wert in der Datei /etc/ssh/sshd_config
`PasswordAuthentication no`

ACHTUNG: SSH Server Restart ist nach Änderung der sshd_config erforderlich