

Inhaltsverzeichnis

- SSH-Key** 3
 - a) Linux Client 3
 - b) Windows Client 3

SSH-Key

Da ich ja ein fauler Mensch bin, nutze ich zum einloggen einen SSH-Key

Diesen kann man unter Linux genauso erstellen wie unter Windows. Hier beide Wege



Aus Sicherheitsgründen nutze ich keinen RSA Key sondern einen ed25519

a) Linux Client

Auf dem Client von dem wir uns auf die Maschine verbinden wollen erstellen wir erstmal das Schlüsselpaar

```
cd ~/.ssh  
ssh-keygen -t ed25519
```

die fragen sollten nun nach seinen eigenen Wünschen beantwortet werden.

Nun kopiere ich den Schlüssel auf den Rechner auf der wir arbeiten wollen

```
ssh-copy-id -i .ssh/id_ed25519.pub  
username_des_Rechners@IP_Adresse_des_Rechners
```

durch den copy Befehl wird es direkt in die authorized_keys eingetragen

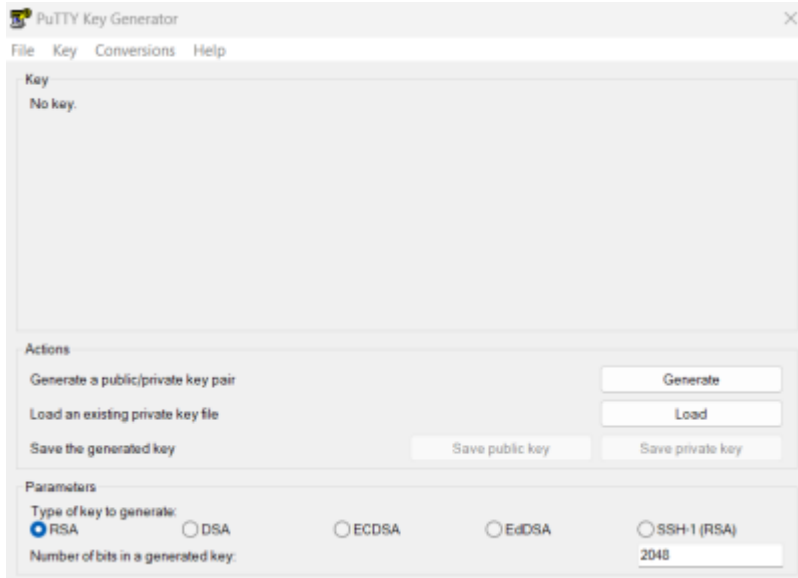
nun können wir uns per SSH dorthin verbinden.

b) Windows Client

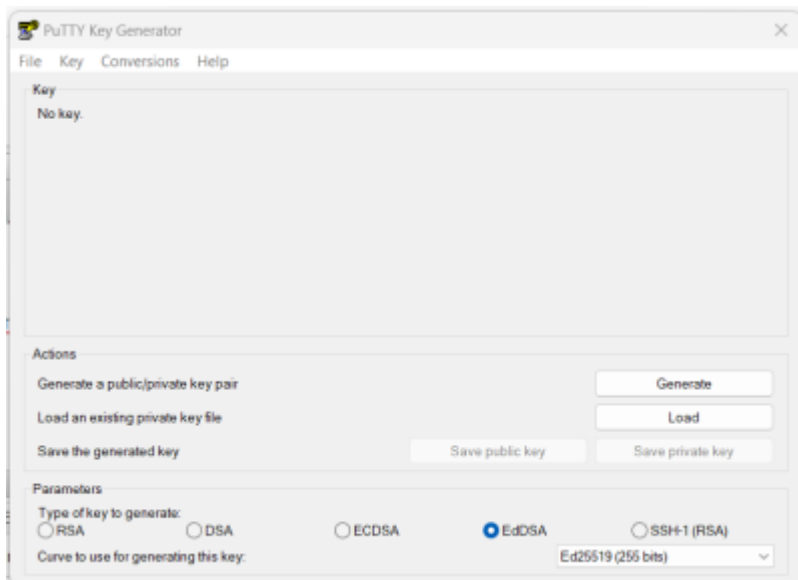
Um per Windows eine SSH Verbindung zu erstellen nutzt ich PuTTY, zu PuTTY gehört auch das Programm PuTTYgen, welches man aber auch einzeln runter laden kann:

<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

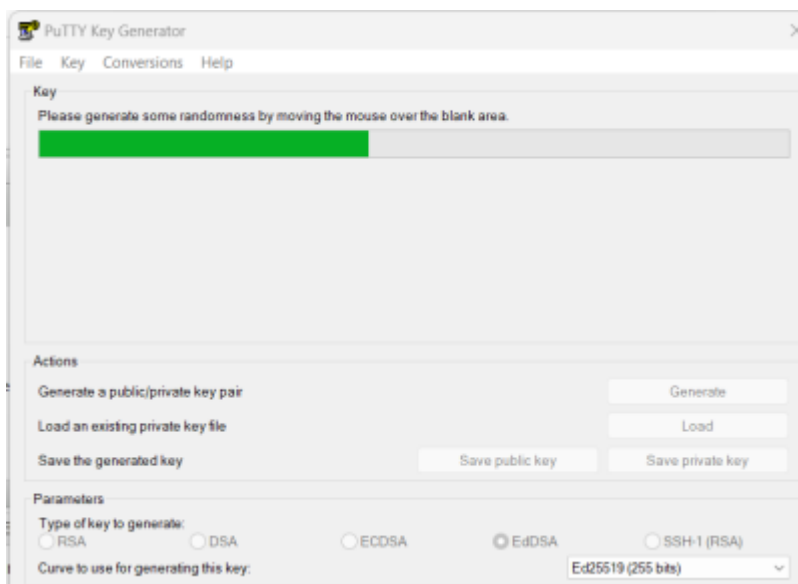
Man startet PuTTYgen



wählt unter Parameters „EdDSA“ und dort „Ed25519“ aus



klickt auf „Generate“ und bewegt entsprechend die Maus, damit der Schlüssel generiert wird.



danach gibt man noch eine Key passphrase ein und speichert den privaten Key als `privat_key.ppk`

Den öffentlichen Key speichert man sich weg, und zwar der Teil der oben im Fenster angezeigt wird.



Dann verbindet man sich per Putty ganz normal mit Benutzer und PW auf den Rechner

nun im Homeverzeichnis des Benutzers legt man den Ordner `.ssh` an

```
mkdir .ssh
```

dann noch ein

```
sudo nano ~/.ssh/authorized_keys
```

oder

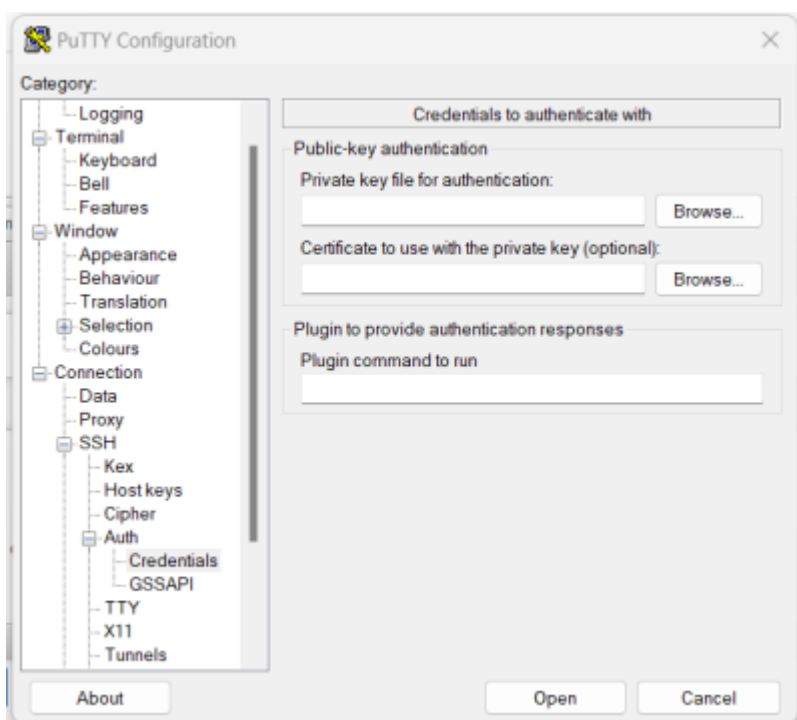
```
sudo vim ~/.ssh/authorized_keys
```

je nachdem was man nutzt bzw. installiert hat

in diese Datei kopiert man den Key aus dem letzten Bild.

Danach kann man unter Putty eine neue Session anlegen und geht auf `Connection>SSH>Auth>Credentials` und hinterlegt den Pfad zum privaten Key, den man ja vorher abgespeichert hat.

Nun kann man sich mit der key Datei anmelden und benötigt nur noch die passphrase so fern eine vergeben wurde.



From:

<https://nas-wiki.hundacker.eu/> - **NAS-Wiki**

Permanent link:

https://nas-wiki.hundacker.eu/doku.php/linux/ssh_key

Last update: **11.03.2024 22:42**

