

Erstellen von SSH Keys

Key generieren (die einfachste Variante)

```
ssh-keygen -C
```

Key generieren im Ed25519 Format (das aktuellste & zZt. sicherste Format)

```
ssh-keygen -o -a 100 -t ed25519 -f ~/.ssh/id_ed25519 -C "name@email.de"
```

Was bedeuten die eben genutzten Parameter?

-o : Speichert den Key im neuen OpenSSH Format anstelle des alten PEM Formats. Muss angegeben werden wenn Ed25519 Keys generiert werden sollen.

-a : Bestimmt die Anzahl der Schlüsselableitungen (engl. KDF - *Key Derivation Function*). Eine höhere Zahl hier sorgt für eine langsamere Überprüfung der Key-Passphrase (Passwort mit dem der Schlüssel zusätzlich geschützt ist) um Brute-Force Angriffe zu erschweren sollte der private Key kompromittiert worden sein.

-t : Legt den Typ des Keys fest der generiert werden soll, in diesem Fall Ed25519. Mögliche Werte hier wären DSA, RSD, ECDSA oder Ed25519.

-f : Legt den Dateinamen des erstellten Keys fest. Soll der Key automatisch vom verwendeten SSH Agent erkannt werden sollte der Default-Pfad `~/.ssh/` beibehalten werden.

-C : Hier kann ein Kommentar angegeben werden. Es gibt keine Vorgabe was hier einzutragen ist, üblicherweise wird der Besitzer des Schlüssels im Format `<username>@<hostname>` hier eingetragen (Bspw. `nielsperetzke@breadfish.de-prod`).

Revision #1

Created 27 September 2021 22:31:58 by nielsperetzke

Updated 29 December 2024 23:24:28 by nielsperetzke