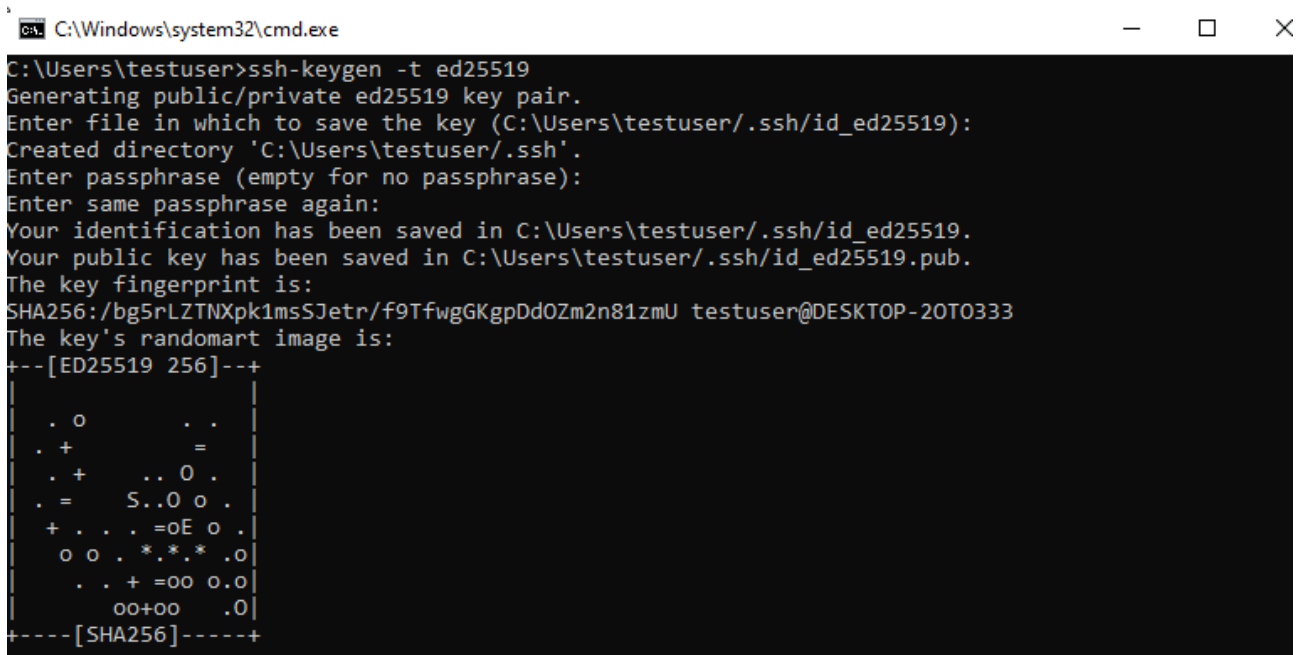


SSH-Shortcuts auf Windows 10+ anlegen

Schritt 1: Key-Paar generieren

Alle Befehle (sofern nicht anders beschrieben) werden auf deinem lokalen Windows-Rechner ausgeführt. Stelle sicher dass du aus allen ssh-Verbindungen rausgegangen bist und dass vor deiner Prompt ein `C:\` zu finden ist.

Der Befehl `ssh-keygen` generiert ein Schlüsselpaar. mit `-t ed25519` kann man die Art der Verschlüsselung auf einen etwas sicheren Typ stellen (Standard ist RSA). Dann wirst du nach dem Dateipfad für den Key gefragt. Hier kannst du einfach `Enter` drücken, um den vorgeschlagenen Pfad zu akzeptieren. Du kannst für deinen Key auch ein Passwort vergeben, so dass man sowohl den Key, als auch das Passwort braucht um sich anzumelden.



```
C:\Windows\system32\cmd.exe
C:\Users\testuser>ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (C:\Users\testuser/.ssh/id_ed25519):
Created directory 'C:\Users\testuser/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\testuser/.ssh/id_ed25519.
Your public key has been saved in C:\Users\testuser/.ssh/id_ed25519.pub.
The key fingerprint is:
SHA256:/bg5rLZTNXpk1msSJetr/f9TfwgGKgpDd0Zm2n81zmU testuser@DESKTOP-20T0333
The key's randomart image is:
+--[ED25519 256]--+
|
|. o          . .
|. +          =
|. +         .. 0 .
|. =         S..0 o .
|. + . . . =oE o .
|. o o . *.*.* .o
|. . + =oo o.o|
|. oo+oo .o|
+-----[SHA256]-----+
```

Schritt 2: SSH-Konfiguration anlegen

Du musst in dem `.ssh` -Verzeichnis unter deinem User-Verzeichnis (idR `C:\Users\<<username>`) eine Datei namens `config` anlegen.

WICHTIG: Diese Datei darf *keine* Datei-Endung wie `.txt` haben! Im Explorer kannst du das sehen indem du bei "Ansicht"->"Optionen"->"Ansicht"->"Erweiterung bei bekannten Dateitypen ausblenden" deaktivierst und dann falls nötig via umbenennen die Endung entfernst.

Im Windows-Terminal kannst du mit `dir` den Verzeichnisinhalt (ähnlich wie `ls -l`) anzeigen und mit `rename` Dateien umbenennen.

```
config - Editor
Datei Bearbeiten Format Ansicht Hilfe
Host gruenau5
  HostName gruenau5.informatik.hu-berlin.de
  User slommage@hu-berlin.de
  IdentityFile ~/.ssh/id_ed25519
Zeile 3, Spalte 28 100% Windows (CRLF) UTF-8
```

Mehr Informationen über die Config-Datei und was man noch so reinschreiben kann gibts in der [Manpage von ssh_config](#)

Schritt 3: Public-Key auf den Server übertragen

Bei der Linux-Anleitung haben wir hier auf `ssh-copy-id` verwiesen, was es unter Windows aber nicht gibt. Stattdessen machen wir die Schritte einfach selbst. Das Ziel ist es, den Inhalt deiner *lokalen* Public-Key-Datei (hat die Endung `.pub`) als neue Zeile in die `~/.ssh/authorized_keys`-Datei *auf dem Server* zu legen.

Wenn du das das erste Mal machst, kannst du einfach den Public-Key per `scp` übertragen und auf dem Server direkt als `authorized_keys` abspeichern.

```
OpenSSH SSH client
C:\Users\testuser>scp ~/.ssh/id_ed25519.pub slommage@hu-berlin.de@gruenau5.informatik.hu-berlin.de:~/.ssh/authorized_keys
slommage@hu-berlin.de@gruenau5.informatik.hu-berlin.de's password:
id_ed25519.pub 100% 107 2.2KB/s 00:00
C:\Users\testuser>ssh gruenau5
Enter passphrase for key 'C:\Users\testuser\~\.ssh\id_ed25519':
Last login: Sun Oct 10 03:12:44 2021 from 95.91.208.130
Have a lot of fun...
slommage@hu-berlin.de@gruenau5:~>
```

Das überschreibt allerdings alles was in der `authorized_keys`-Datei vorher drin war und deshalb solltest du, wenn du das nicht willst, stattdessen den Public-Key so wie er ist auf den Server kopieren und dann auf dem Server (also nachdem du `ssh` gemacht hast) zB. per `cat meinkey.pub >> ~/.ssh/authorized_keys` zur Liste hinzufügen.

Hinweis: Es kann sein, dass der `~/.ssh`-Ordner auf dem Server noch nicht existiert und deshalb `scp` einen Fehler ausgibt. In diesem Fall musst du dich nochmal normal mit `ssh username@hu-berlin.de@gruenau5.informatik.hu-berlin.de` einloggen und mit `mkdir` das Verzeichnis auf dem Server erstellen. Beende die SSH-Verbindung mit `exit` und probiere den `scp`-Befehl nochmal.

Schritt 4: ???

Schritt 5: Profit

Jetzt kannst du dich mit einem einfachen `ssh gruenau5` auf dem Server einloggen und Benutzername und genauer Server, sowie auch der Key der verwendet werden soll werden aus der Konfigurationsdatei gelesen.

Wenn du andere Kürzel für andere gruenaus einrichten möchtest, musst du nur neue Abschnitte in der `config`-Datei anlegen, indem du den bestehenden Abschnitt kopierst, darunter einfügst und dann den Kürzelnamen und den Ziel-Server anpasst. Da der Key zwischen allen Uni-Servern synchronisiert wird, musst du ihn nicht neu erstellen oder auf den Server kopieren.

Wenn du auf Probleme stößt, kannst du auch im Internet nach Anleitungen wie dieser suchen.