Anlegen von SSH Schlüsseln

Um unter Windows sowohl einen ED25519- als auch einen RSA-SSH-Schlüssel zu erzeugen, gehst du am besten folgendermaßen vor:

---

1. Voraussetzungen

- **Windows 10 (ab Version 1803) oder Windows 11** – hier ist der OpenSSH-Client bereits integriert.
- **PowerShell** oder **Eingabeaufforderung**, idealerweise als Administrator gestartet (für Agent-Konfiguration).

---

2. Öffne PowerShell

1. Klicke auf **Start** → tippe **PowerShell** → **Rechtsklick** → **Als Administrator ausführen**.
2. Wechsel (falls gewünscht) in dein Benutzer-.ssh-Verzeichnis:

   ```
   cd $HOME\.ssh
   ```

   > **Hinweis:** Falls das Verzeichnis noch nicht existiert, leg es an mit `mkdir $HOME\.ssh`.

---

3. Erzeugen eines ED25519-Schlüssels

1. Führe den Befehl aus:

```
ssh-keygen -t ed25519 -C "dein.comment@beispiel.de"
```

2. Du wirst gefragt nach:
   - **Dateiname** (Standard: `%USERPROFILE%\.ssh\id_ed25519`) → einfach mit **Enter** bestätigen, falls du den Standard willst.
   - **Passphrase** (optional): Tipp eine starke Passphrase ein oder leer lassen → Enter.

Dadurch erhältst du:

- **Privat-Key:** `%USERPROFILE%\.ssh\id_ed25519`
- **Public-Key:** `%USERPROFILE%\.ssh\id_ed25519.pub`

---

4. Erzeugen eines RSA-Schlüssels

1. Führe den Befehl aus:

```
ssh-keygen -t rsa -b 4096 -C "dein.comment@beispiel.de"
```

2. Abfragen:
   - **Dateiname** (Standard: `%USERPROFILE%\.ssh\id_rsa`) → Enter.
   - **Passphrase** (empfohlen): Eingeben oder leer lassen → Enter.

Erzeugt:

- **Privat-Key:** `%USERPROFILE%\.ssh\id_rsa`
- **Public-Key:** `%USERPROFILE%\.ssh\id_rsa.pub`

---

5. SSH-Agent starten und Schlüssel laden (optional)

Damit du nicht bei jeder SSH-Verbindung dein Passwort eingeben musst, kannst du den **ssh-agent** nutzen:

1. Starte den Agent:

```
Start-Service ssh-agent
```

2. Konfiguriere ihn so, dass er immer startet:

```
Set-Service -Name ssh-agent -StartupType Automatic
```

3. Lade deine Schlüssel in den Agenten:

```
ssh-add $HOME\.ssh\id_ed25519
ssh-add $HOME\.ssh\id_rsa
```

Du wirst nach den Passphrasen gefragt (falls gesetzt).

---

6. Public Key auf dem Server hinterlegen

1. Zeige den Public Key an:

```
type $HOME\.ssh\id_ed25519.pub
# bzw.
type $HOME\.ssh\id_rsa.pub
```

2. Kopiere die Ausgabe und füge sie in `~/.ssh/authorized_keys` auf deinem Ziel-Server ein.

Zusammenfassung der Befehle

```
# 1. .ssh-Verzeichnis anlegen (falls nötig)
mkdir $HOME\.ssh

# 2. ED25519-Schlüssel
ssh-keygen -t ed25519 -C "dein.comment@beispiel.de"

# 3. RSA-Schlüssel (4096 Bit)
ssh-keygen -t rsa -b 4096 -C "dein.comment@beispiel.de"

# 4. SSH-Agent starten & Schlüssel hinzufügen
Start-Service ssh-agent
Set-Service -Name ssh-agent -StartupType Automatic
ssh-add $HOME\.ssh\id_ed25519
ssh-add $HOME\.ssh\id_rsa
```

```
# 5. Public Key anzeigen
type $HOME\.ssh\id_ed25519.pub
type $HOME\.ssh\id_rsa.pub
```

Damit hast du unter Windows erfolgreich sowohl einen ED25519- als auch einen RSA-SSH-Schlüssel erstellt und bereitgestellt. Viel Erfolg beim Einrichten deiner SSH-Verbindungen!

Revision #2
Created 9 June 2025 07:48:32 by Stefan Mechler
Updated 9 June 2025 07:49:10 by Stefan Mechler