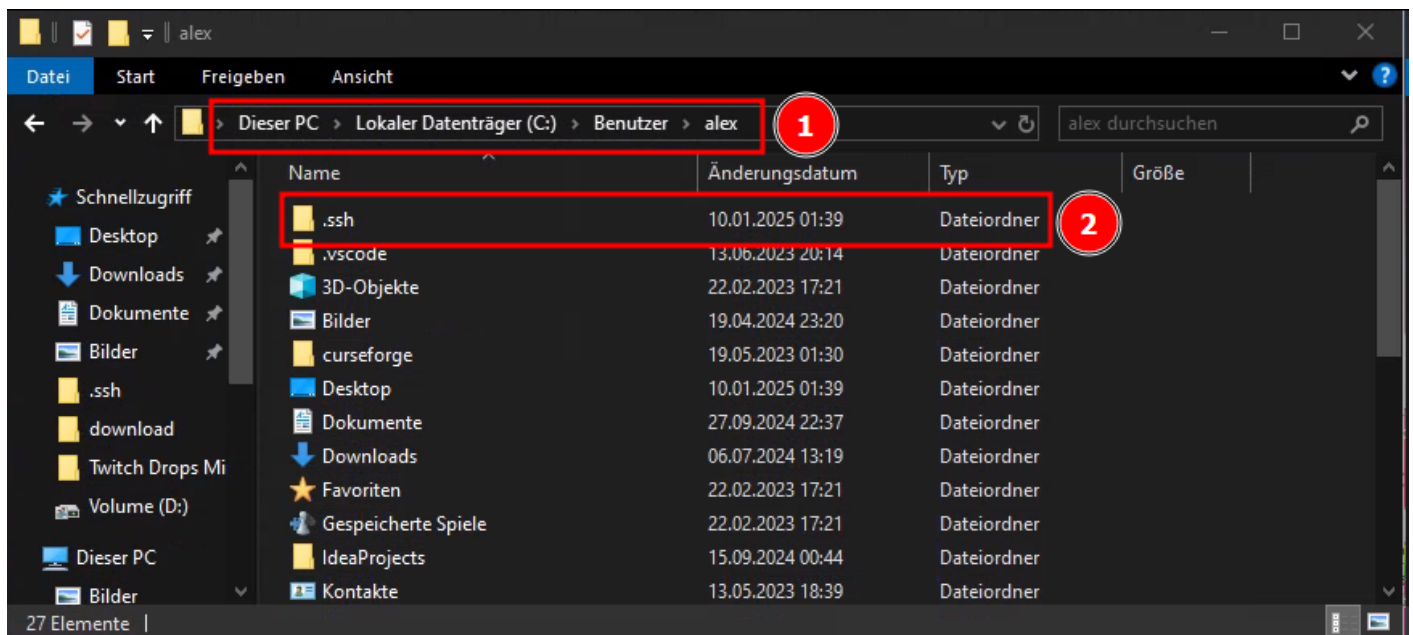


# SSH-Key erstellen und einrichten

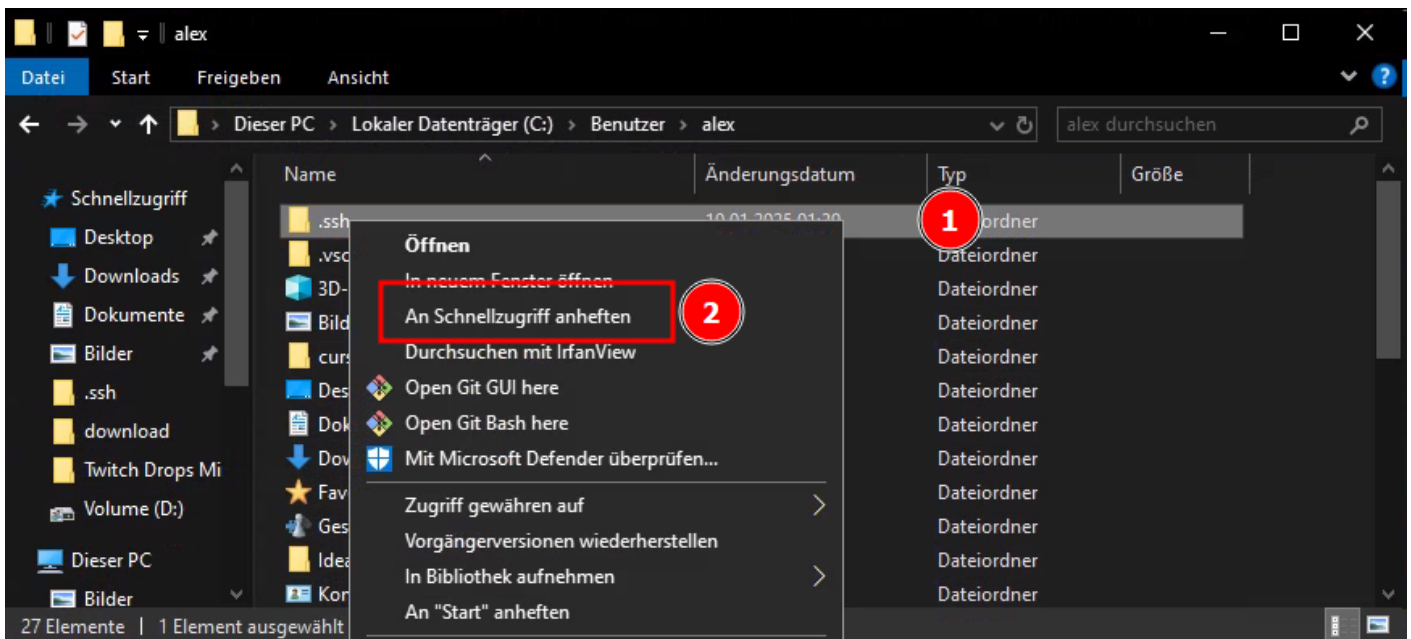
Teil 1 und Teil 2 müssen vorher gemacht werden!

## 1. Vorbereitung

1. Geh in deinen Benutzer Ordner unter `C:\Users\DEIN-BENUTZER`
2. Lege den Ordner `.ssh` an

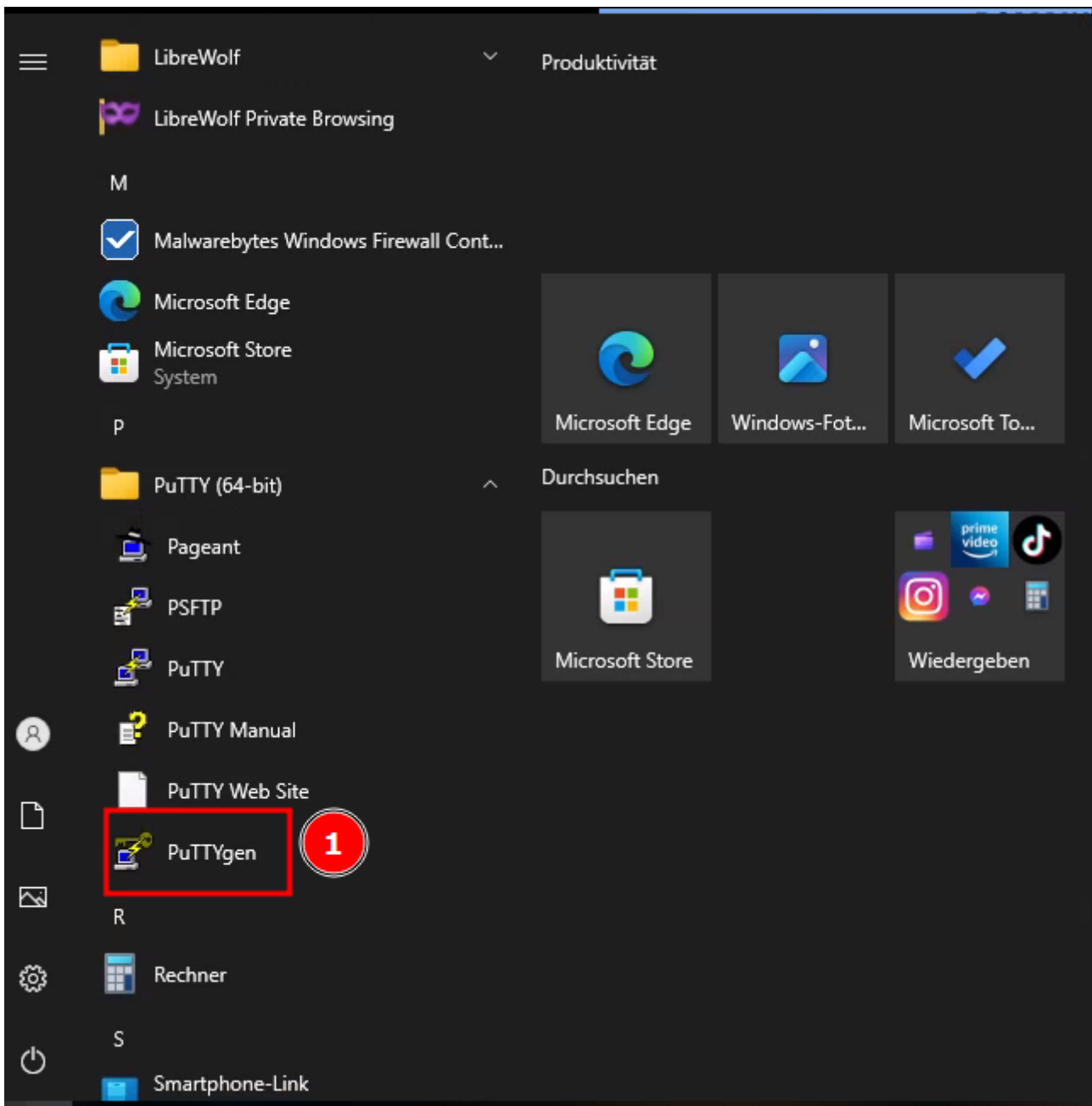


1. Anschließend den Ordner per Rechtsklick auswählen
2. Mit **An Schnellzugriff anheften** Links hinzufügen

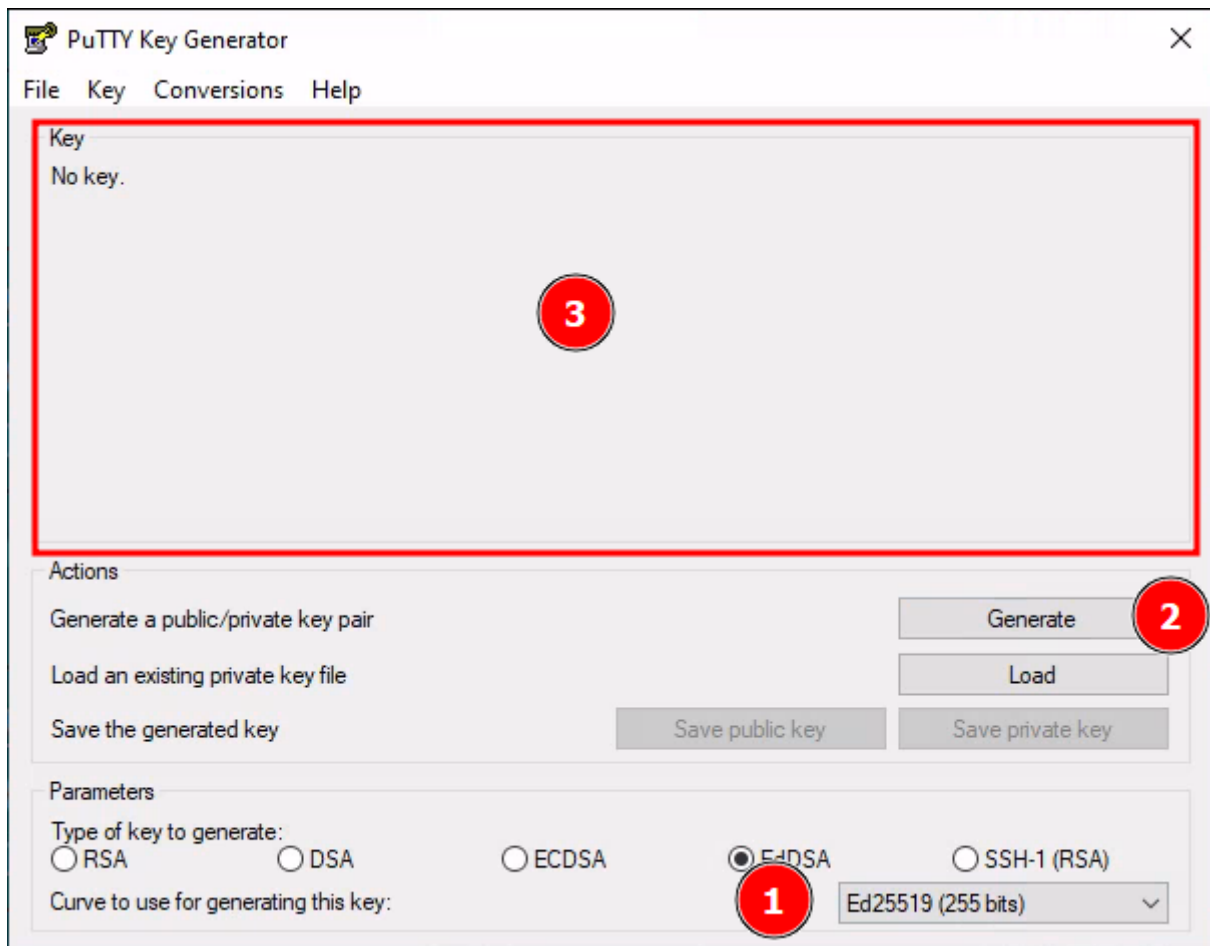


## 2. Schlüssel Erstellung

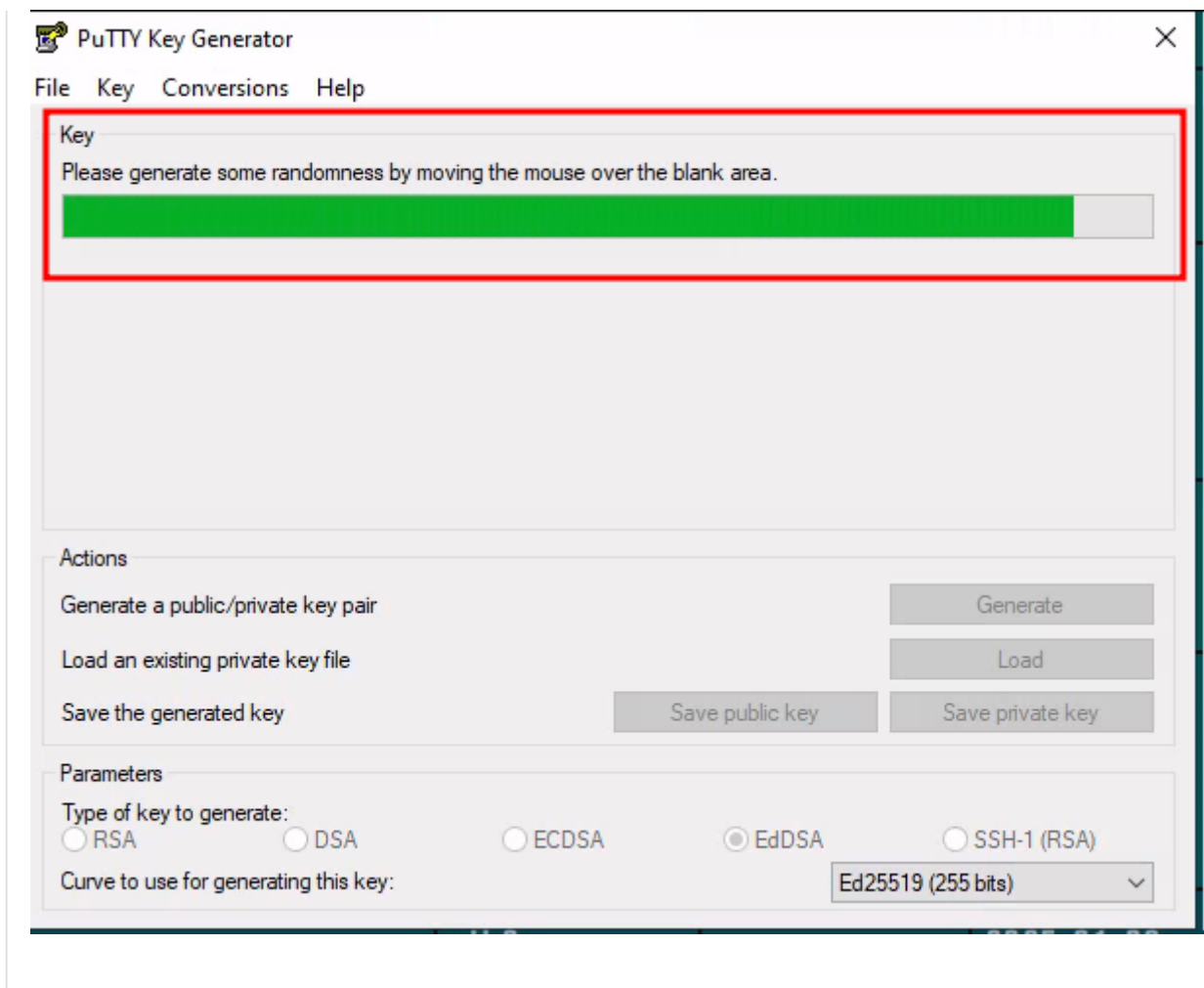
1. Dann wird PuTTYgen gestartet



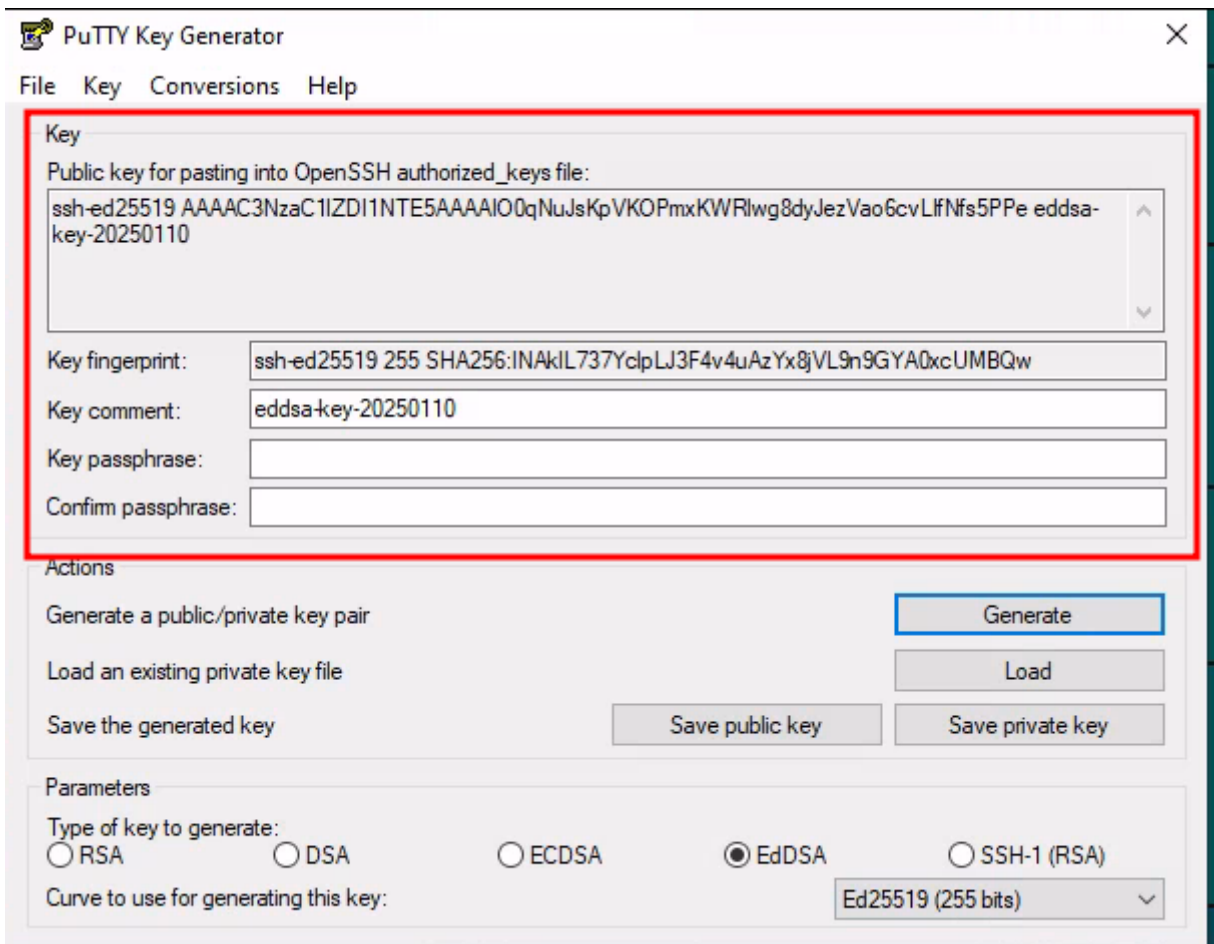
1. Dann wird auf den Schlüsseltyp **EdDSA** gestellt
2. Mit Generate starten wir die Generation
3. Maus in dem Feld solange bewegen bis Text erscheint



## Generationsfortschritt




Der Schlüssel ist fertig wenn das Fenster so aussieht:



Jetzt den erzeugten Schlüssel 3 mal speichern

## Speichern des Putty Private Keys

Auf "Save private key" klicken

 PuTTY Key Generator ×

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized\_keys file:

```
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIO0qNuJsKpVKOPmxKWRlwg8dyJezVao6cvLifNfs5PPe eddsa-key-20250110
```

Key fingerprint: ssh-ed25519 255 SHA256:INakIL737YclpLJ3F4v4uAzYx8jVL9n9GYA0xcUMBQw

Key comment: eddsa-key-20250110

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

Save the generated key Save public key Save private key 1

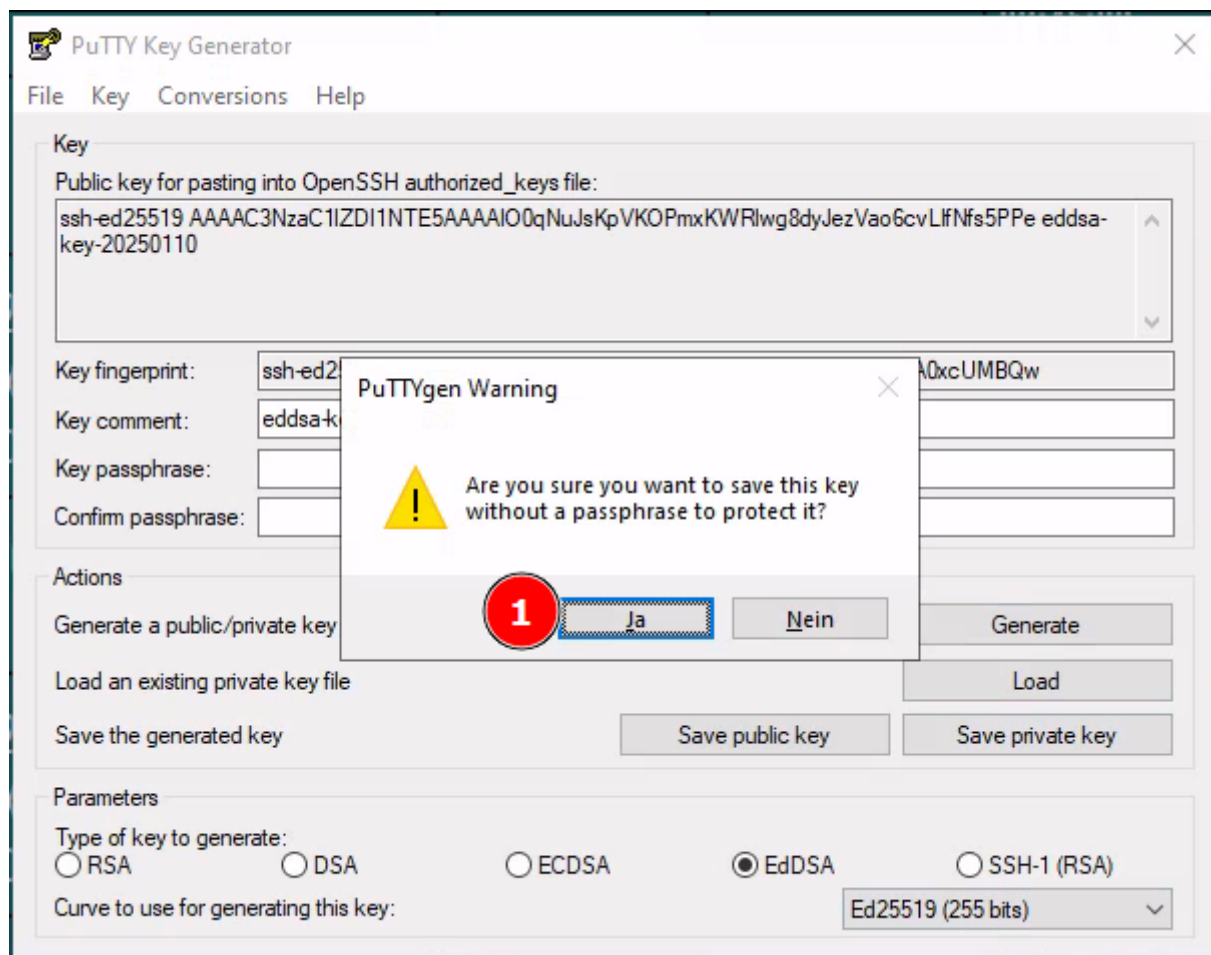
Parameters

Type of key to generate:

☐ RSA ☐ DSA ☐ ECDSA ☒ EdDSA ☐ SSH-1 (RSA)

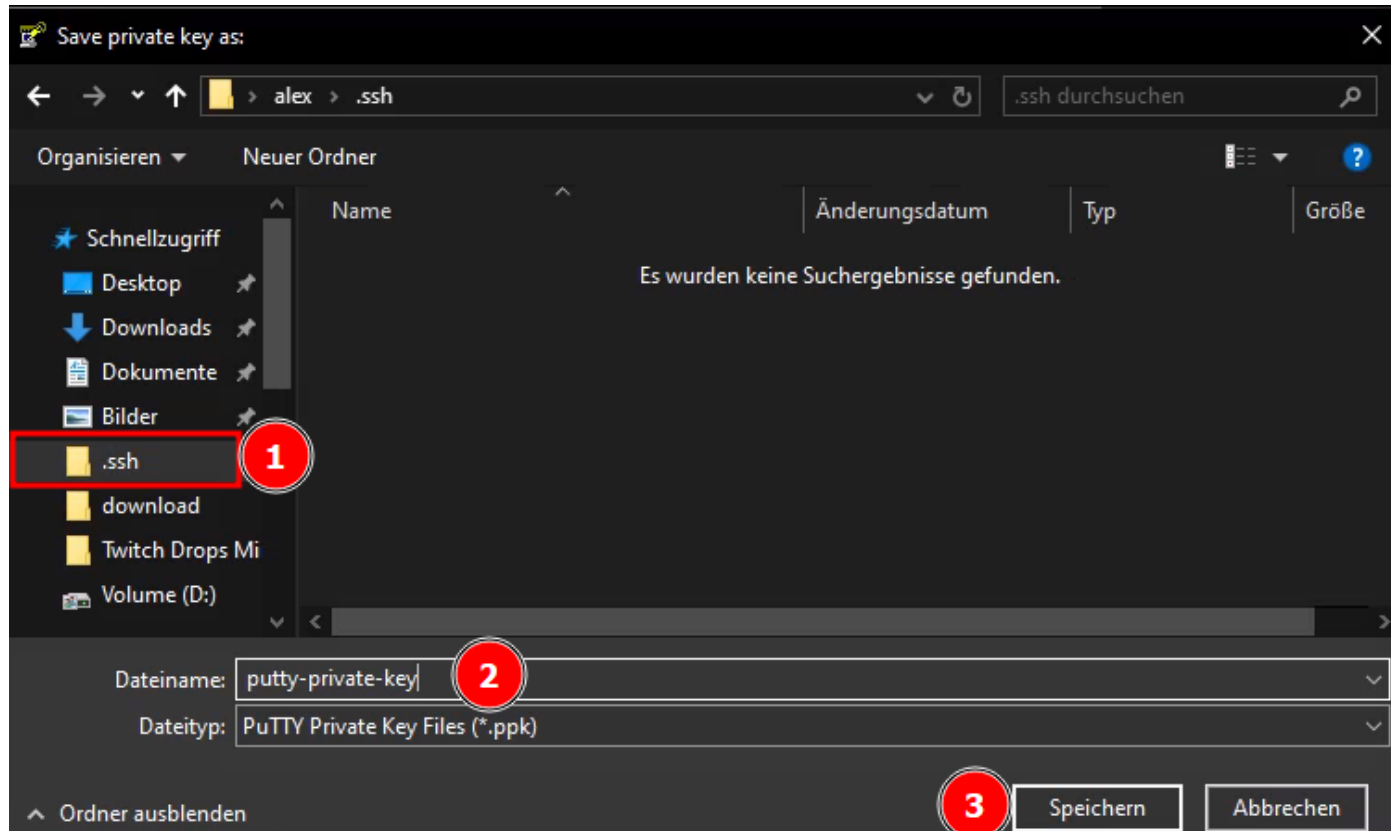
Curve to use for generating this key: Ed25519 (255 bits) ▼

Dialog mit Ja bestätigen



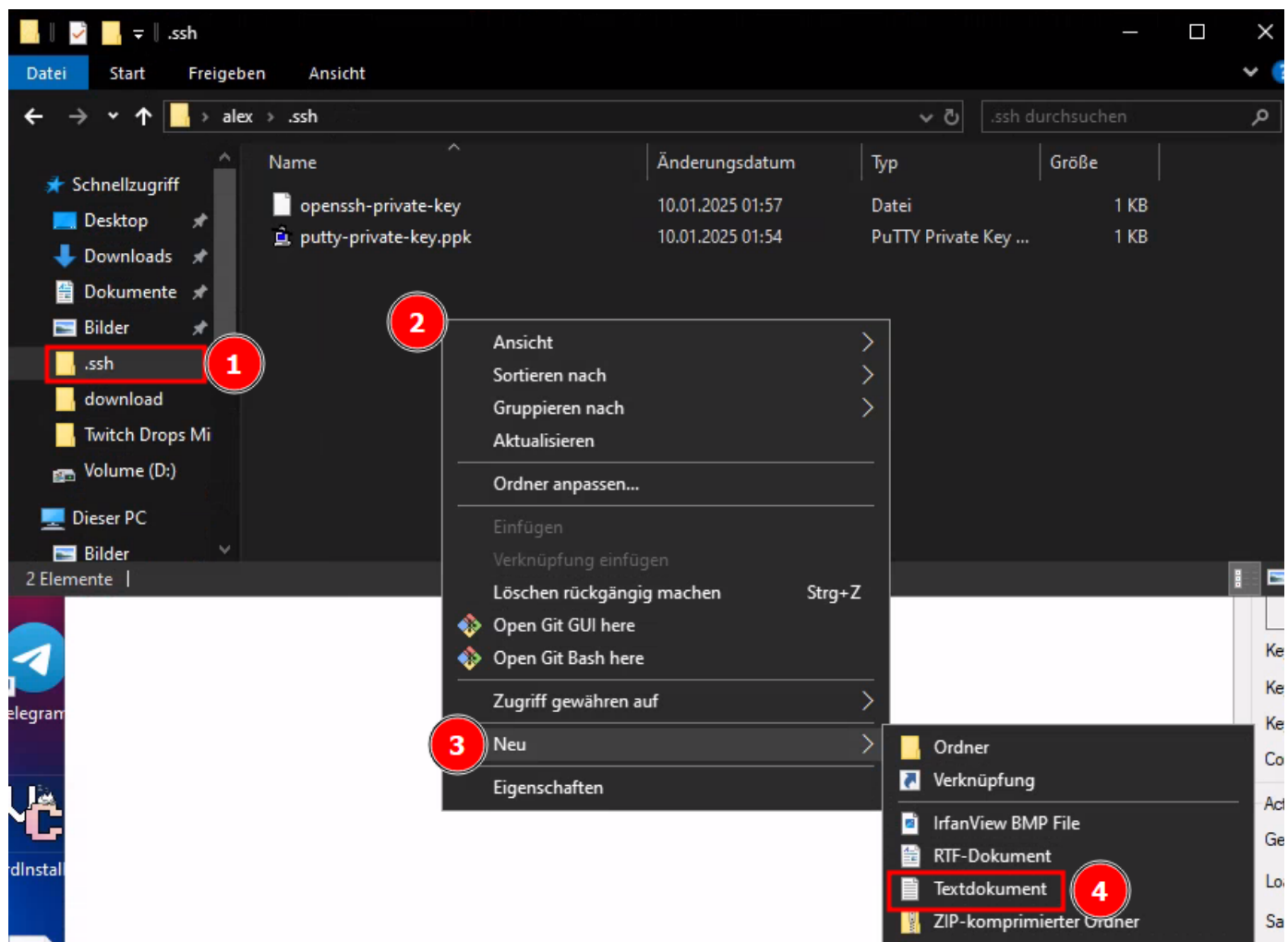
1. Auf `.ssh` klicken
2. Bei Dateinamen `putty-private-key` eintragen
3. Und auf `Speichern` klicken



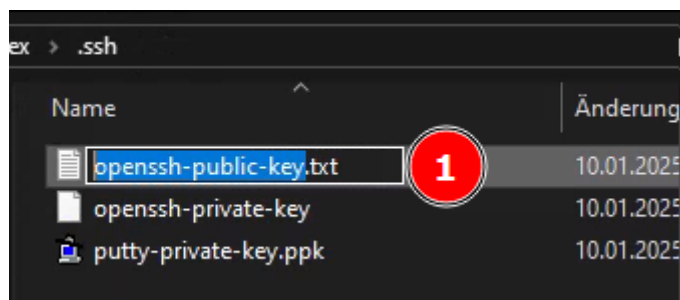


## Speichern des OpenSSH Public Keys

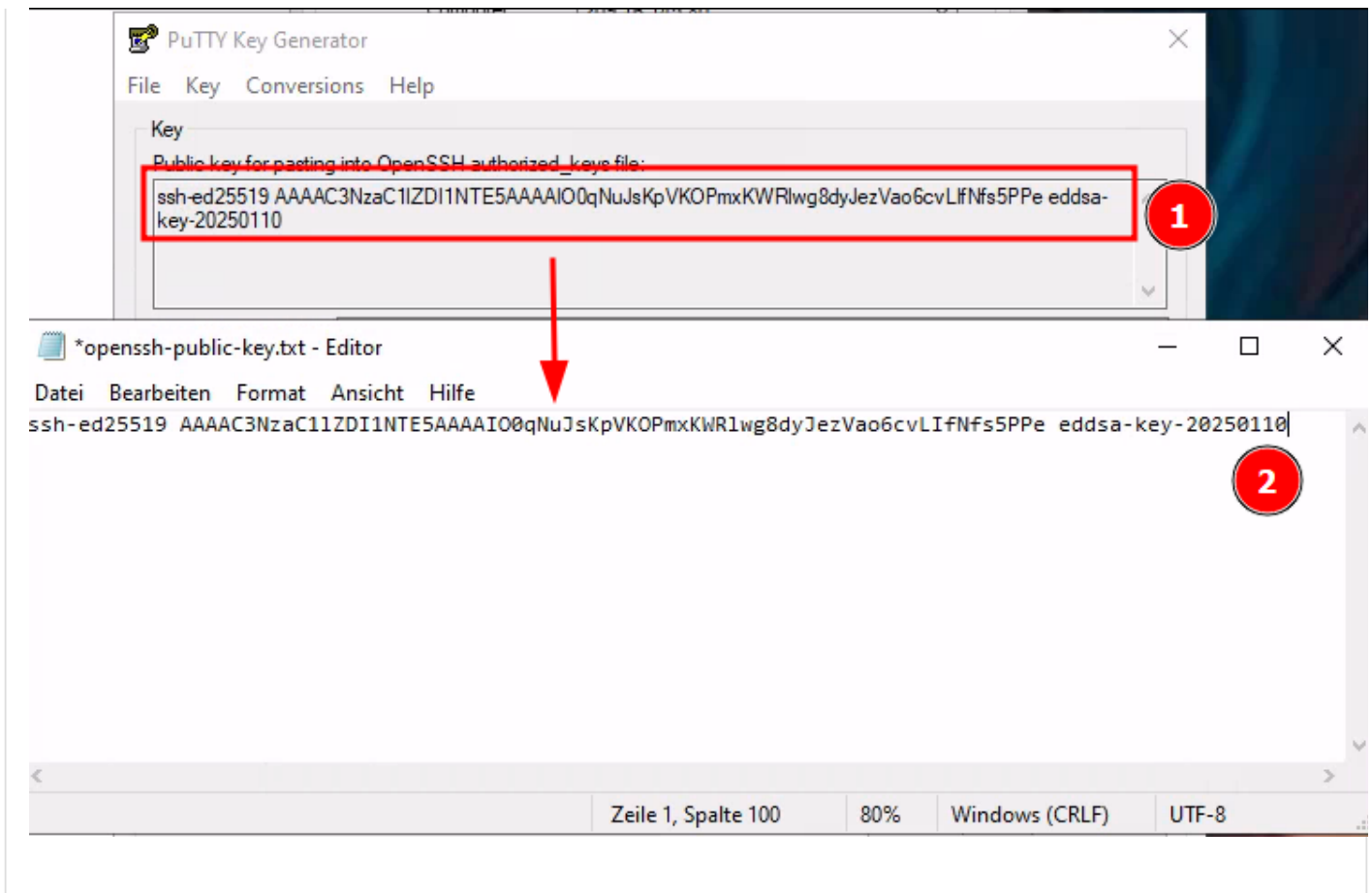
0. Den **Windows Explorer** öffnen
1. Auf **.ssh** klicken
2. Rechtsklick
3. Auf **Neu** gehen
4. **Textdokument** auswählen



1. Die Datei **openssh-public-key.txt** nennen und mit Doppelklick öffnen

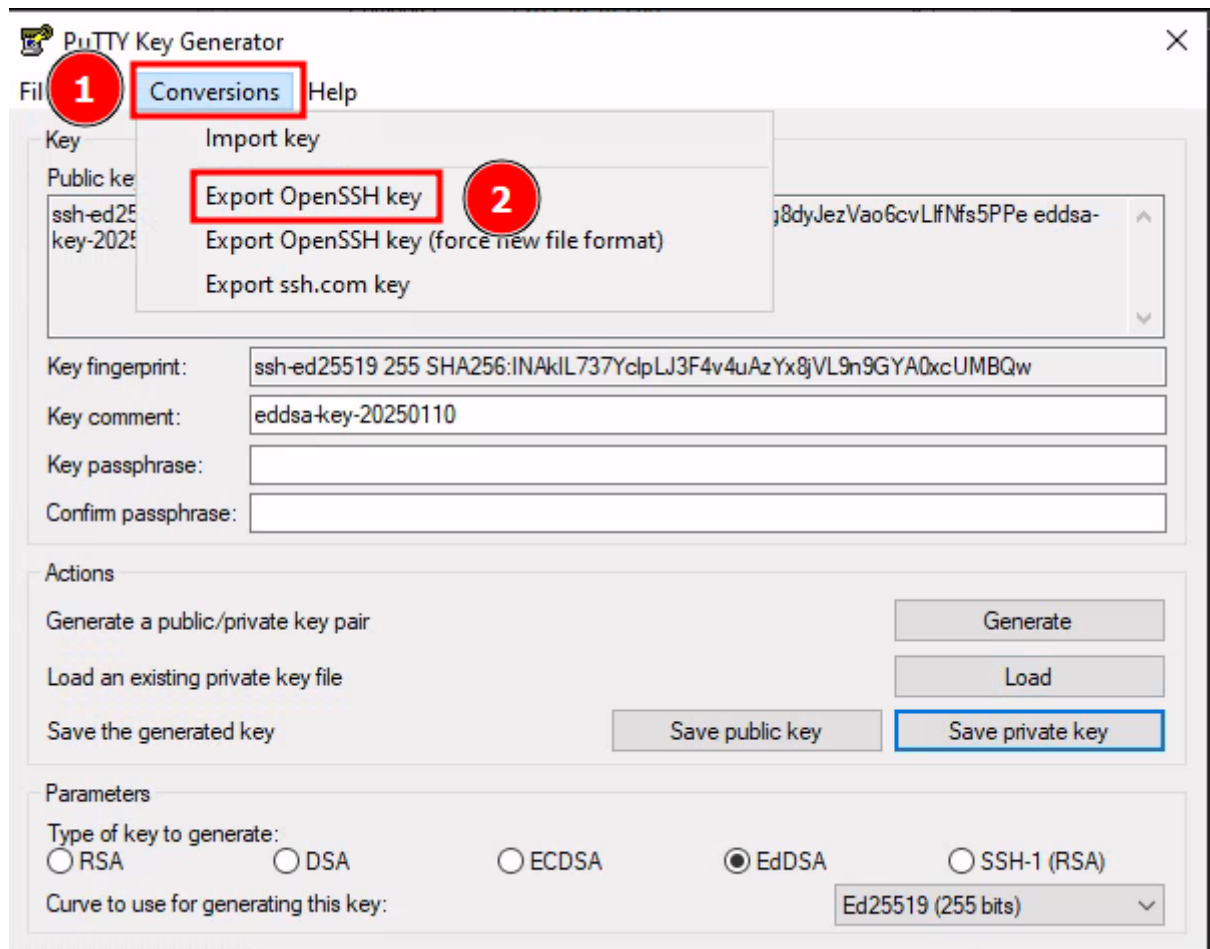


1. Den Inhalt aus dem Textfeld im **PuTTYgen** kopieren
2. In den Editor einfügen und speichern

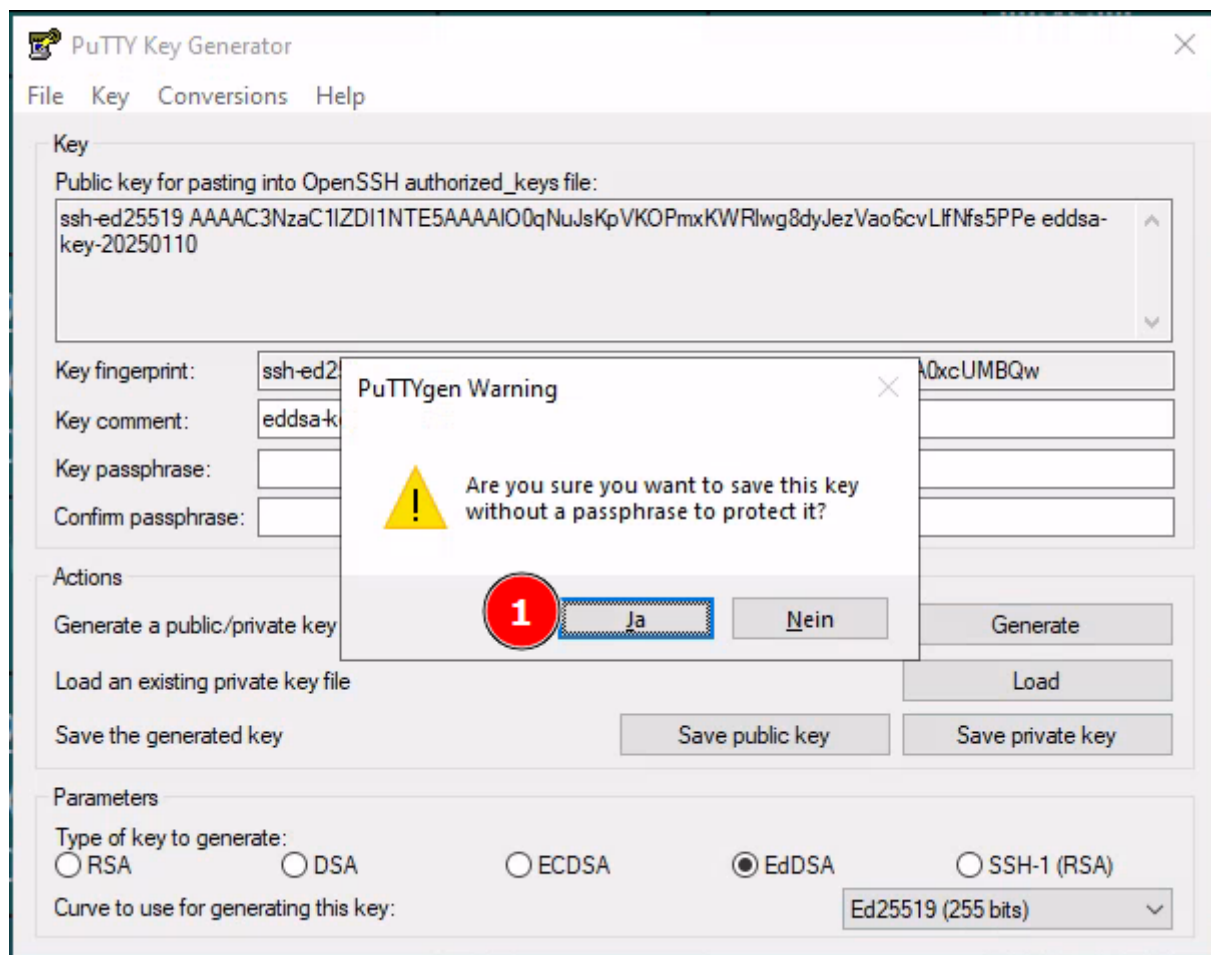


## Speichern des OpenSSH Private Keys

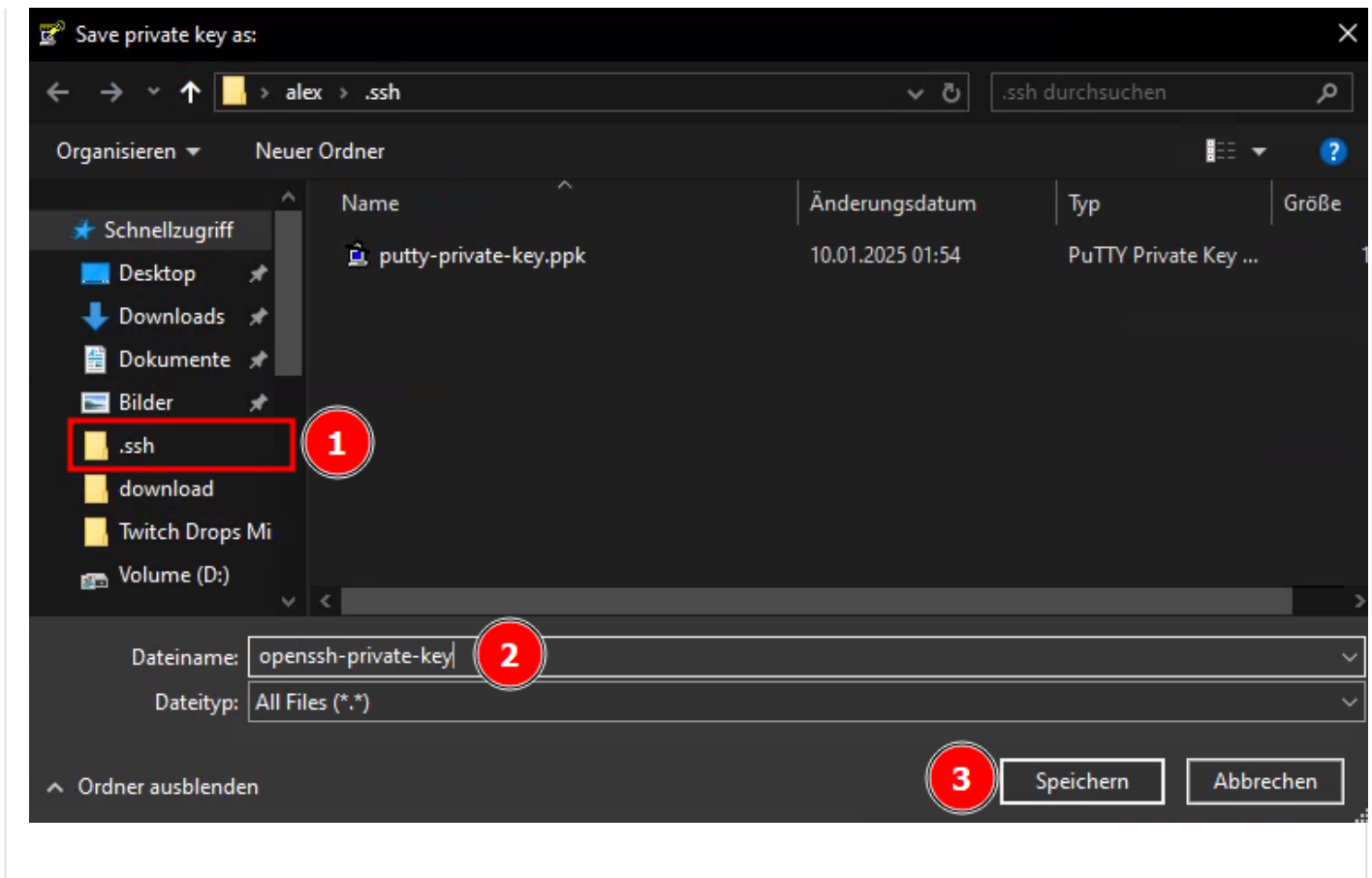
1. Auf Conversion klicken
2. Auf Export OpenSSH key klicken



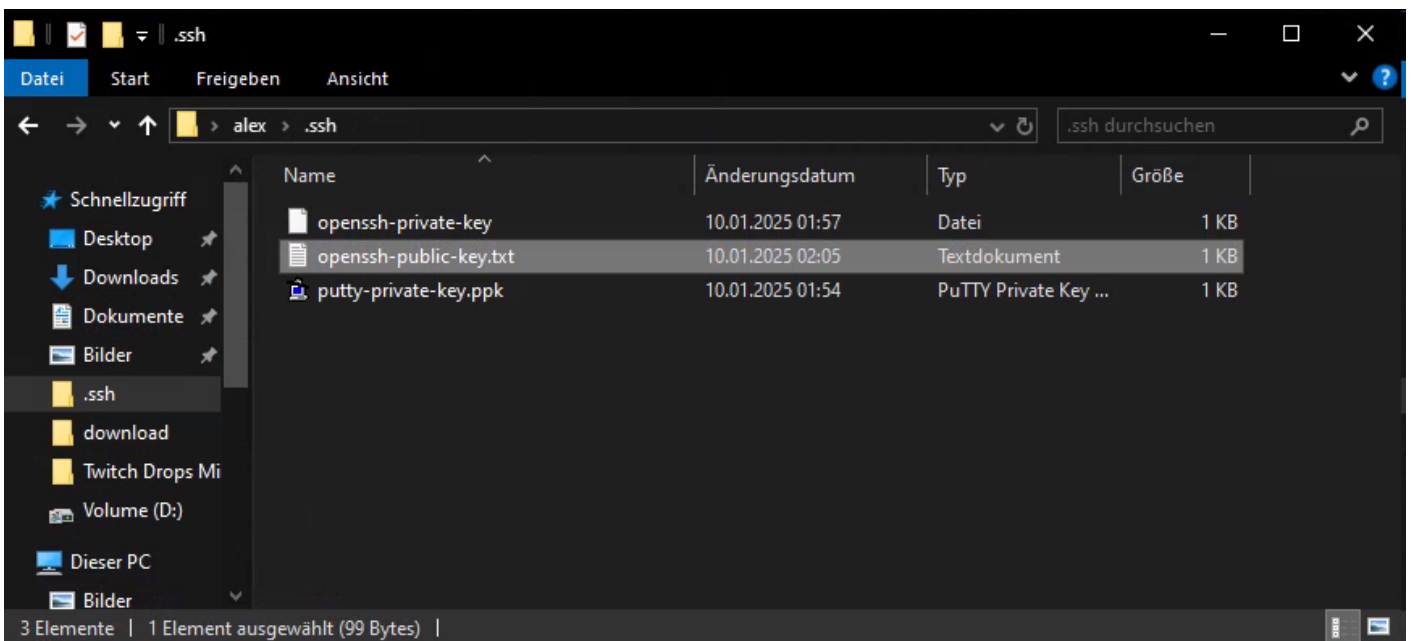
Dialog mit Ja bestätigen



1. Auf `.ssh` klicken
2. Bei Dateinamen `openssh-private-key` eintragen
3. Und auf `Speichern` klicken



Jetzt sollten im .ssh Ordner diese 3 Dateien liegen:



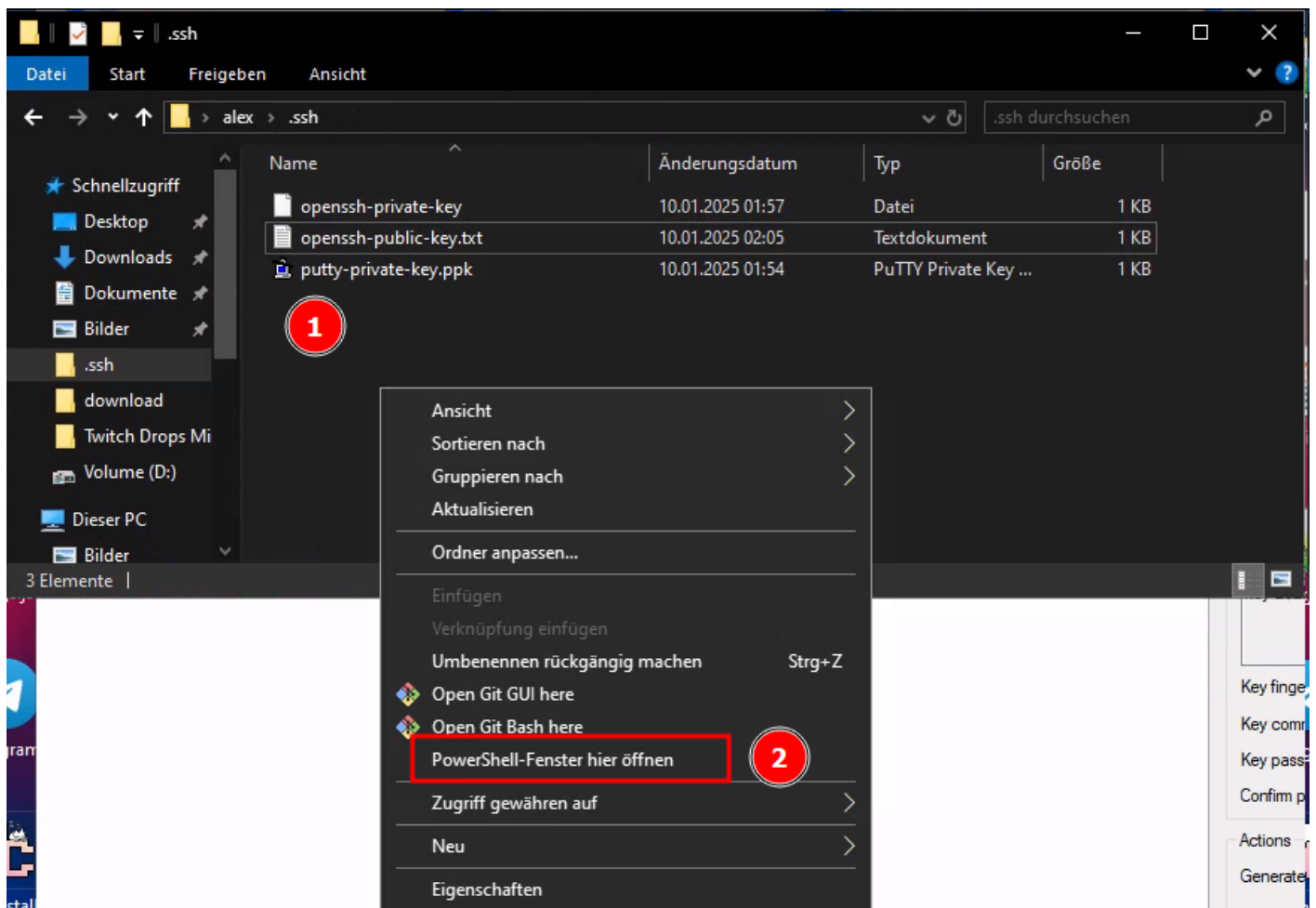
Den **putty-private-key.ppk** darf man nicht verlieren da aus ihm die anderen beiden Dateien wieder erstellt werden können.

Weder der **putty-private-key.ppk** noch der **openssh-private-key** dürfen an andere Personen weitergegeben werden! Man gibt ja die Login Daten fürs Onlinebanking auch nicht weiter oder?

Wenn euch jemand nach eurem **SSH-Key** fragt gebt ihr entweder die **openssh-public-key.txt** weiter oder deren Inhalt

### 3. Schlüssel registrieren

1. Mit Shift+Rechtsklick das Erweiterte Kontext Menü aufrufen
2. PowerShell-Fenster hier öffnen auswählen



Folgendes in der PowerShell ausführen:

```
ssh-add .\openssh-private-key
```



```
Windows PowerShell
PS C:\Users\alex\.ssh> ssh-add .\openssh-private-key_
```

Wenn ihr folgende Ausgabe bekommt

```
Windows PowerShell
PS C:\Users\alex\.ssh> ssh-add .\openssh-private-key
Bad permissions. Try removing permissions for user: DESKTOP-AFH52IH\
\herter (S-1-5-21-605832379-3039829534-2830679314-1005) on file C:/U
sers/alex/.ssh/openssh-private-key.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@           WARNING: UNPROTECTED PRIVATE KEY FILE!           @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions for '.\openssh-private-key' are too open.
It is required that your private key files are NOT accessible by oth
ers.
This private key will be ignored.
```

Müsst ihr folgenden Befehl ausführen:

```
$p = ".\openssh-private-key"; icacls.exe $p /reset; icacls.exe $p /GRANT:R "$($env:USERNAME):(R)"; icacls.exe
$p /inheritance:r; ssh-add $p
```

Wenn ihr die folgende Ausgabe bekommt wurde der Schlüssel richtig geladen:

```
Windows PowerShell
PS C:\Users\alex\.ssh> $p = ".\openssh-private-key"; icacls.exe $p /reset; icacls.exe $p /GRANT:R "$($env:US
ERNAME):(R)"; icacls.exe $p /inheritance:r; ssh-add $p
Bearbeitete Datei: .\openssh-private-key
1 Dateien erfolgreich verarbeitet, bei 0 Dateien ist ein Verarbeitungsfehler aufgetreten.
Bearbeitete Datei: .\openssh-private-key
1 Dateien erfolgreich verarbeitet, bei 0 Dateien ist ein Verarbeitungsfehler aufgetreten.
Bearbeitete Datei: .\openssh-private-key
1 Dateien erfolgreich verarbeitet, bei 0 Dateien ist ein Verarbeitungsfehler aufgetreten.
Identity added: .\openssh-private-key (eddsa-key-20250110)
PS C:\Users\alex\.ssh>
```

## 4. Kontrolle

Zum Abschluss folgendes in der PowerShell ausführen zur Kontrolle: ssh-add -L und man sieht das der Schlüssel geladen ist:

```
Windows PowerShell
PS C:\Users\alex\.ssh> ssh-add -L
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIO0qNuJsKpVKOPmxKWRlwg8dyJezVao6cvLIIfNfs5PPe eddsa-key-20250110
PS C:\Users\alex\.ssh>
```

Jetzt könnt ihr beim Login per SSH als Authentifizierung "Agent" verwenden so euer Public key im Server hinterlegt ist.



Version #4

Erstellt: 10 Januar 2025 01:16:19 von craftman96

Zuletzt aktualisiert: 10 Januar 2025 14:00:46 von craftman96