

Windows PuTTY SSH-Client



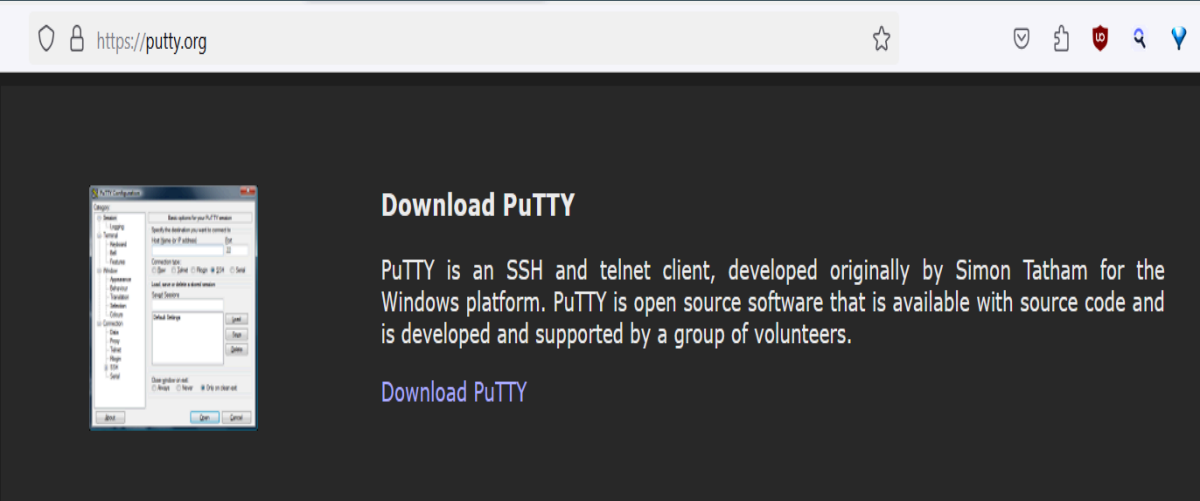
Inhaltsverzeichnis

- [Der PuTTY SSH-Client](#)
- [Download und -Installation](#)
- [Verbindung zum remote Host](#)
- [Passwortloses Login mit PuTTY - Überblick](#)
- [PuTTYGen: Schlüsselpaar erzeugen](#)
- [Remote Host: Public Key bekannt machen](#)
- [PuTTY: Private Key bekannt machen](#)
- [Links](#)

Der PuTTY SSH-Client

- PuTTY ist seit Jahren ein beliebter SSH-Client für Windows.
- PuTTY ist ein grafischer SSH-Client, der auch Telnet, Rlogin und serielle Verbindungen unterstützt. Die Konfiguration erfolgt über ein GUI. Erst bei Öffnen der `ssh`-Verbindung wird ein Terminal-Fenster geöffnet.
- PuTTY als kann `msi`-Datei von <https://www.putty.org/> heruntergeladen und dann mit einem windows-typischen Installationsprozess installiert werden.

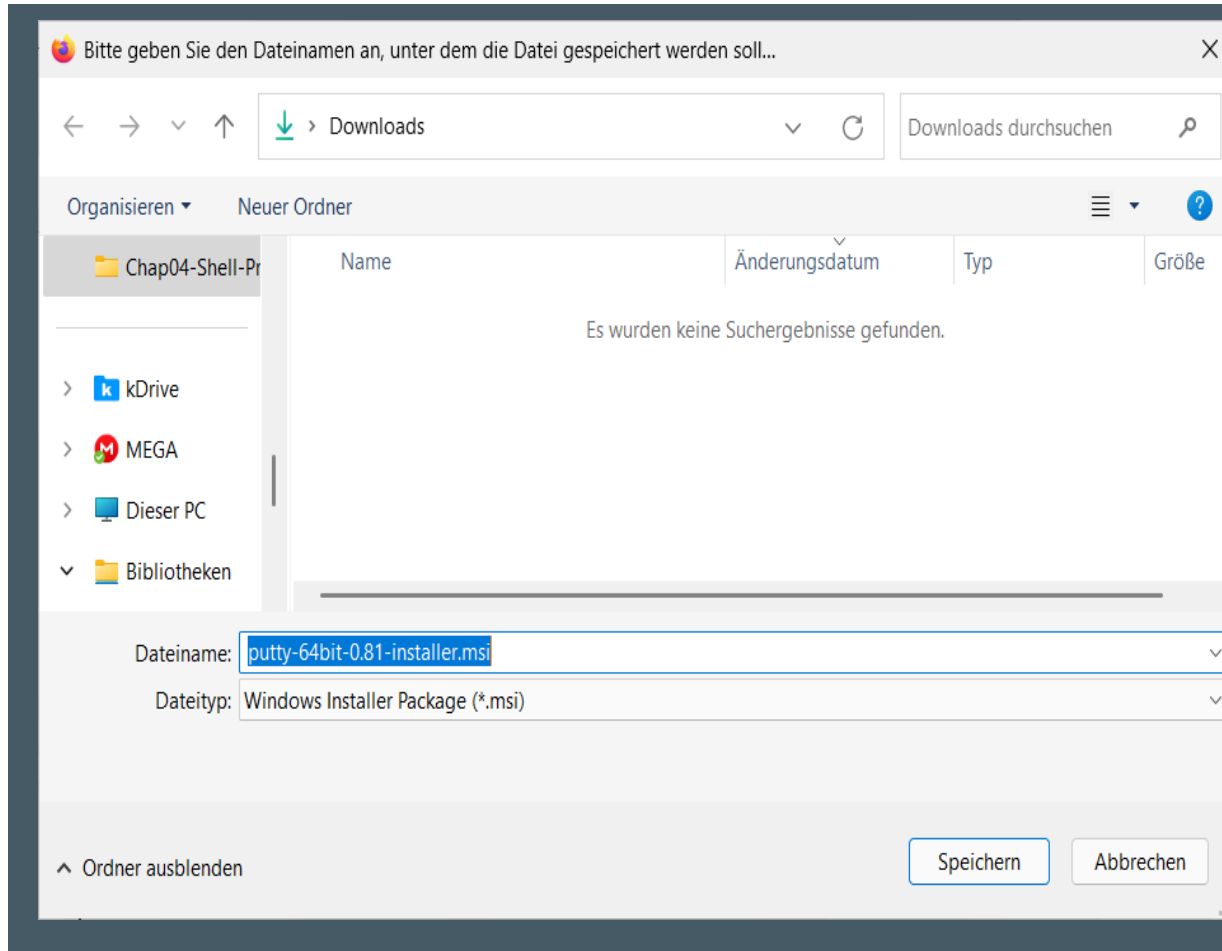
Download und -Installation



Download von

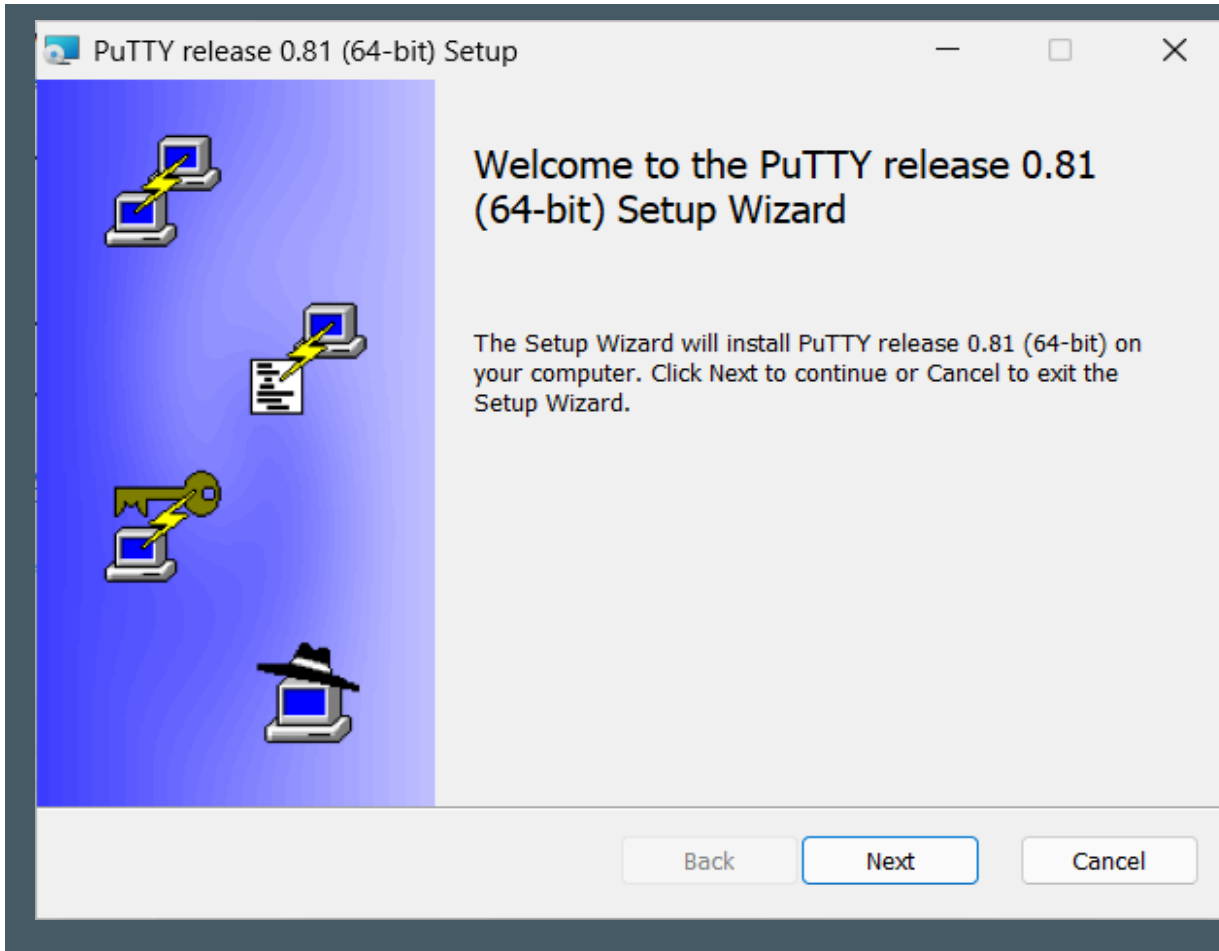
<https://www.putty.org/>

msi -Setup-Datei speichern



Download: msi -Setup-Datei
speichern

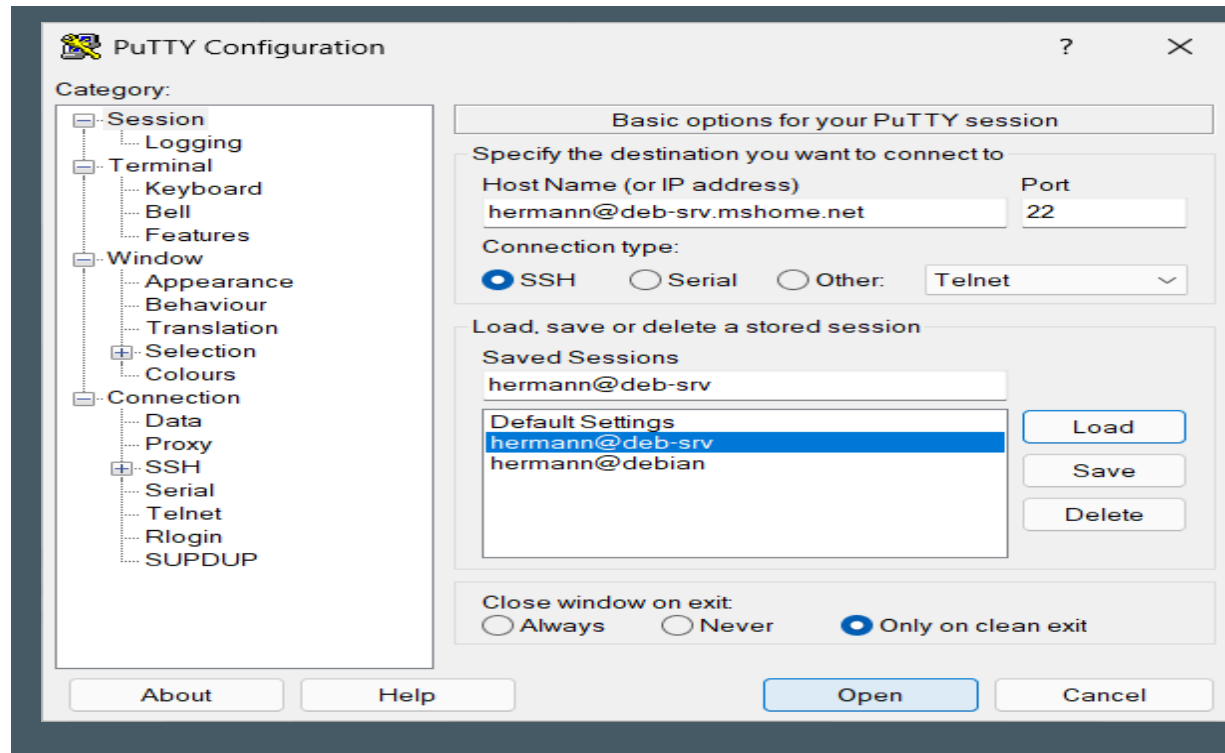
msi -Setup-Datei ausführen



**Start des
Installationsprozesses**

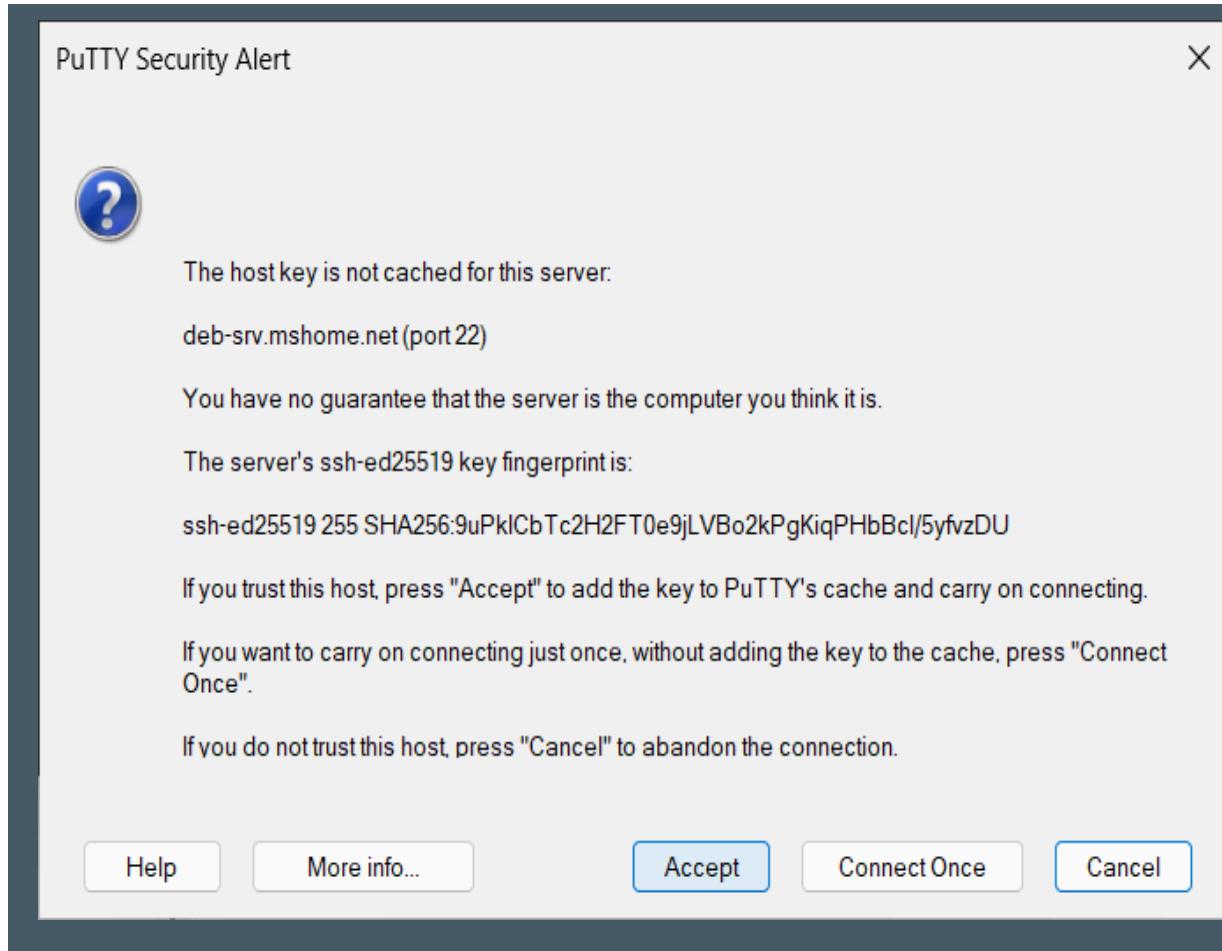
Verbindung zum remote Host

Einstellen der Verbindungsparameter



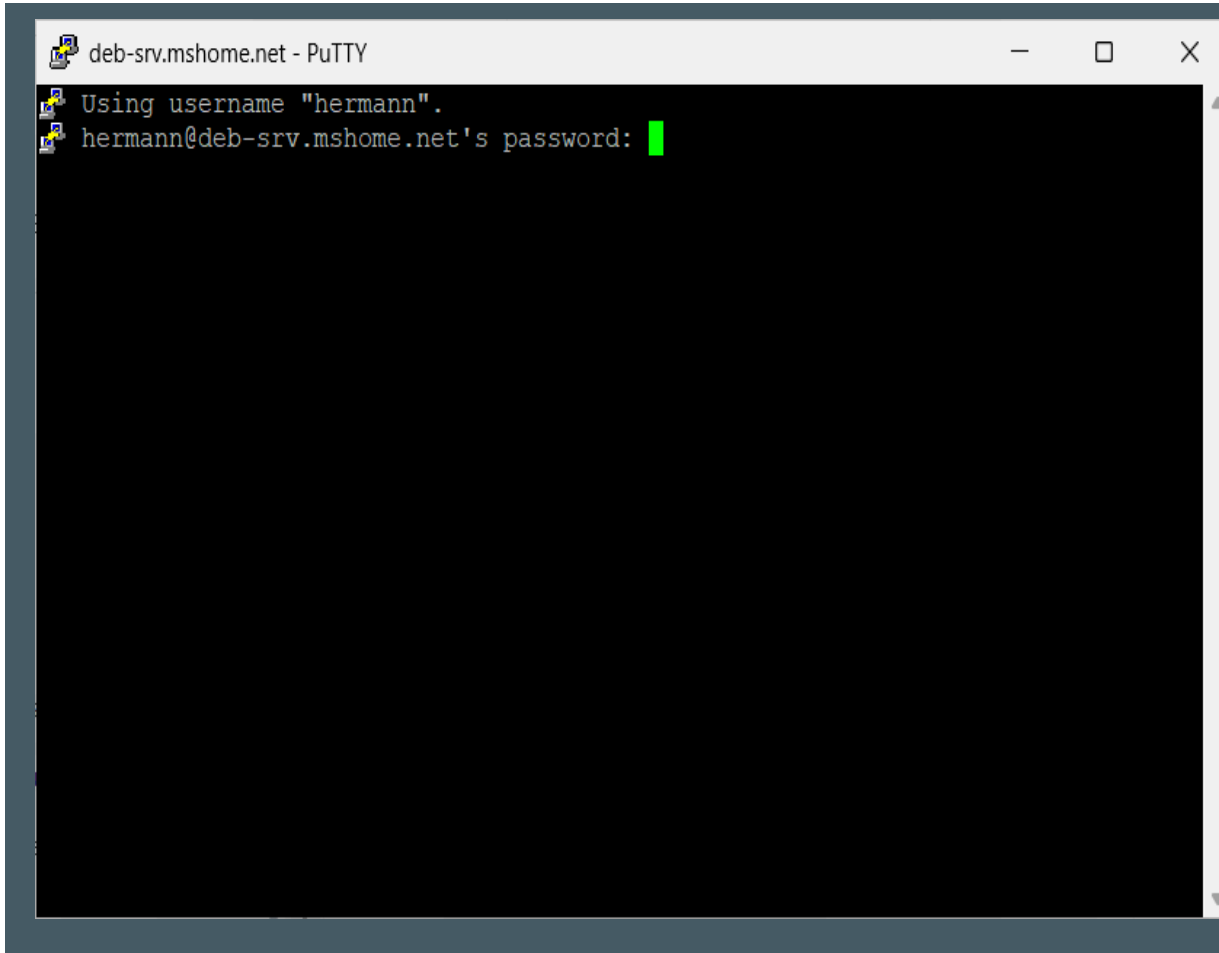
**Benutzer, Host und Port
eintragen, mit "Save"
speichern und mit "Open"
die Verbindung aufbauen**

Fingerabdruck des remote Host



**Fingerabdruck des Hosts
bestätigen mit "Accept"**

Login auf dem remote Host



The screenshot shows a PuTTY terminal window titled "deb-srv.mshome.net - PuTTY". The terminal output displays the message "Using username 'hermann'." followed by the prompt "hermann@deb-srv.mshome.net's password:". A green cursor is positioned at the end of the password prompt, indicating where the user should enter their password.

**Beim Login Passwort
eingeben**

Eingeloggt auf dem remote Host

```
hermann@deb-srv: ~  
Using username "hermann".  
hermann@deb-srv.mshome.net's password:  
Linux deb-srv 6.1.0-28-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.119-1 (2024-11-22)  
) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Wed Dec  4 17:59:45 2024 from 172.29.144.1  
hermann@deb-srv:~$
```

**Begrüßung nach
erfolgreichem Login**

Passwortloses Login mit PuTTY - Überblick

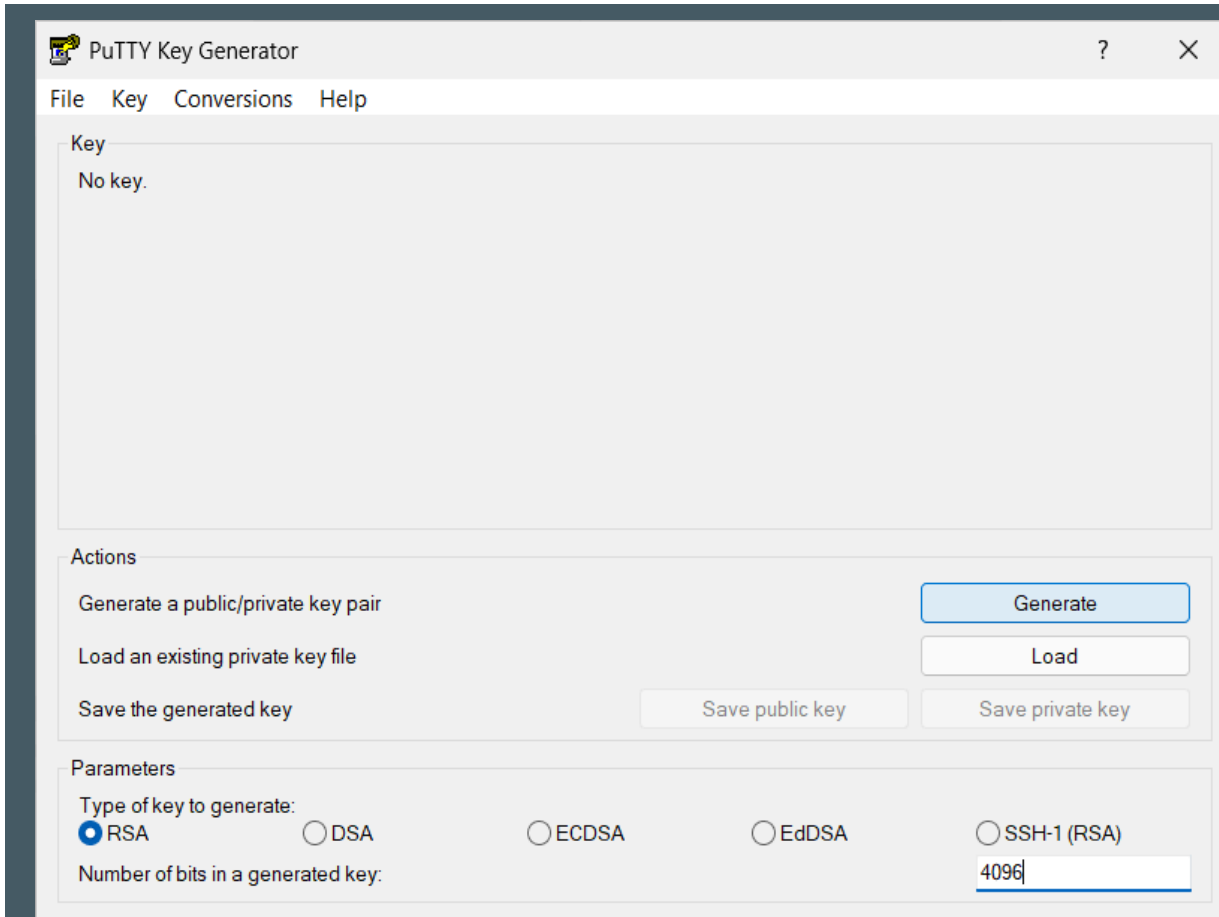
- Mit dem begleitenden Programm `PuTTYgen` kann ein Schlüsselpaar erzeugt werden.
- Der öffentliche Schlüssel wird auf dem entfernten Host in die Datei `~/.ssh/authorized_keys` eingetragen.
- Der private wird als Datei mit dem Suffix `.ppk` gespeichert.
- Er kann dann in PuTTY als Authentifizierungsmethode für die Verbindung ausgewählt oder in einem Verbindungsprofil gespeichert werden.
- Auf den folgenden Folien ist die Anleitung dazu mit Screenshots.

PuTTYGen: Schlüsselpaar erzeugen

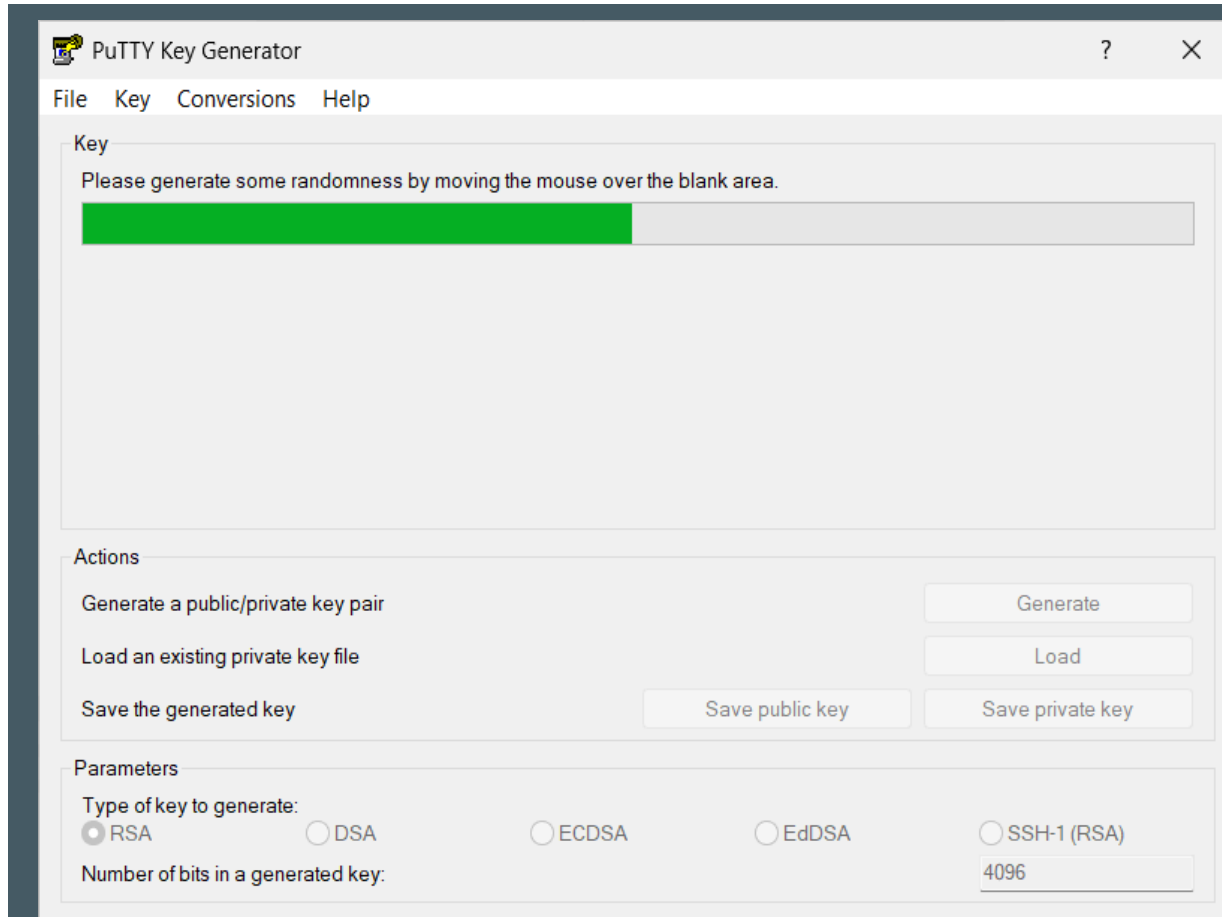
- Mit PuTTYGen wird ein Schlüsselpaar erzeugt.
- Die Passphrase lassen wir leer (in einer Testumgebung vertretbar)
- Der private Schlüssel wird gespeichert, hier unter `.ssh-putty\id_rsa.ppk`. Der Dateiname muss das Suffix `.ppk` haben.
- Der öffentliche Schlüssel wird unter `.ssh-putty\id_rsa.pub` gespeichert. (Der Verzeichnisname ist frei wählbar. Hier wurde er `ssh-putty` genannt.)
- Der öffentliche Schlüssel wird kopiert, um ihn danach auf dem entfernten Host in die Datei `~/.ssh/authorized_keys` einzufügen.

Schlüsselpaar erzeugen

**Verschlüsselungsalgorithmus
(RSA) und Schlüssellänge
(4096 Bit) auswählen, dann
Klick auf "Generate"**

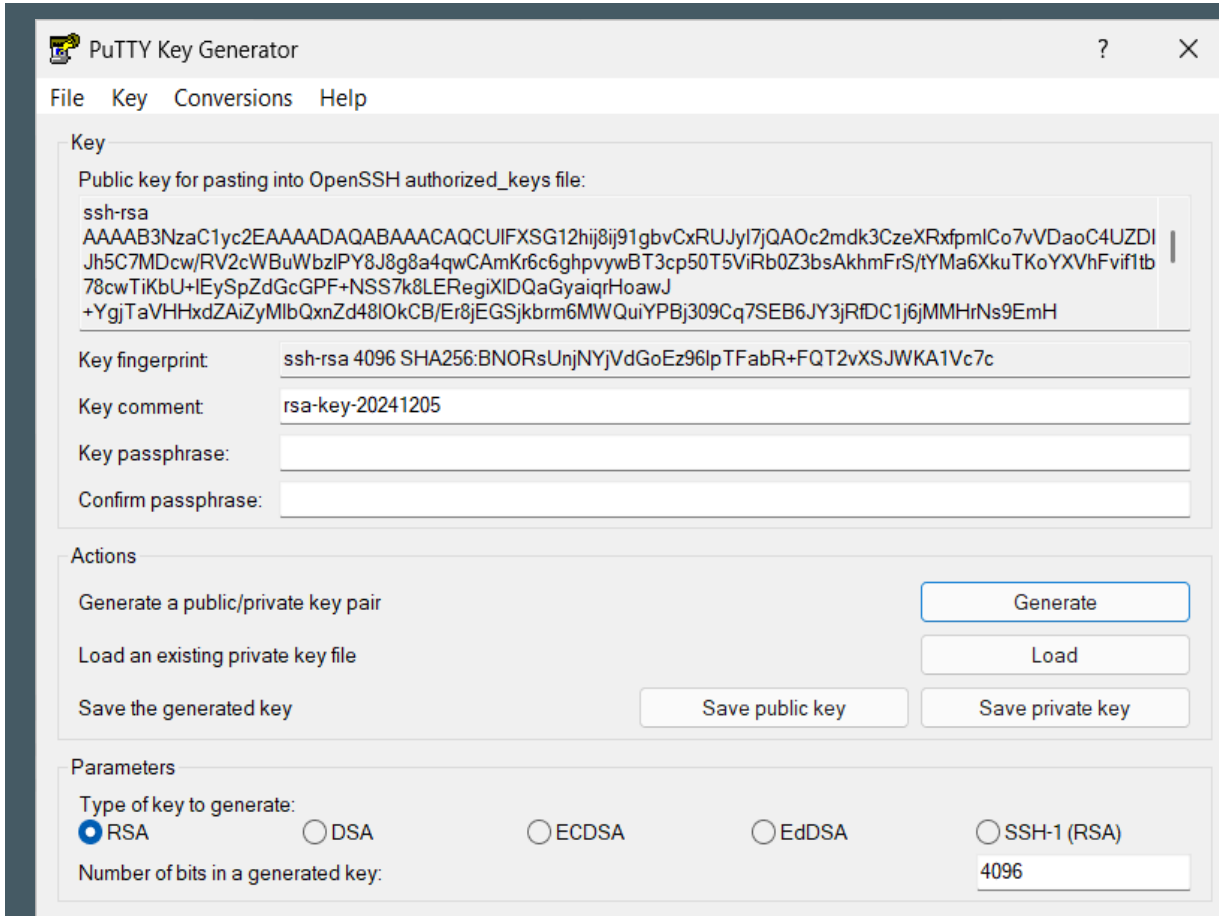


Schlüsselgenerierung



**Mit Mausbewegungen den
Zufallsgenerator
unterstützen**

Schlüsselpaar erzeugt



The screenshot shows the PuTTY Key Generator application window. The 'Key' tab is active, displaying the generated public key in a text area. Below the text area, the key fingerprint and comment are shown. The 'Actions' section contains buttons for generating, loading, and saving keys. The 'Parameters' section shows the key type set to RSA and the number of bits set to 4096.

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQCUiFXSG12hij8ij91gbvCxRUJyl7jQA0c2mdk3CzeXRxfpmlCo7vVDaoC4UZDI
Jh5C7MDcw/RV2cWBUWbzIPY8J8g8a4qwCAmKr6c6ghpvywBT3cp50T5ViRb0Z3bsAkHmFrS/tYMa6XkuTKoYXVhFvif1tb
78cwTiKbU+IEySpZdGcGPF+NSS7k8LERegiXIDQaGyaiqrHoawJ
+YgjTaVHHxdZAiZyMlbQxnZd48IOkCB/Er8jEGSjkbrm6MWQuiYPBj309Cq7SEB6JY3jRfDC1j6jMMHrNs9EmH
```

Key fingerprint: ssh-rsa 4096 SHA256:BNORsUnjNYjVdGoEz96lpTFabR+FQT2vXSJWKA1Vc7c

Key comment: rsa-key-20241205

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

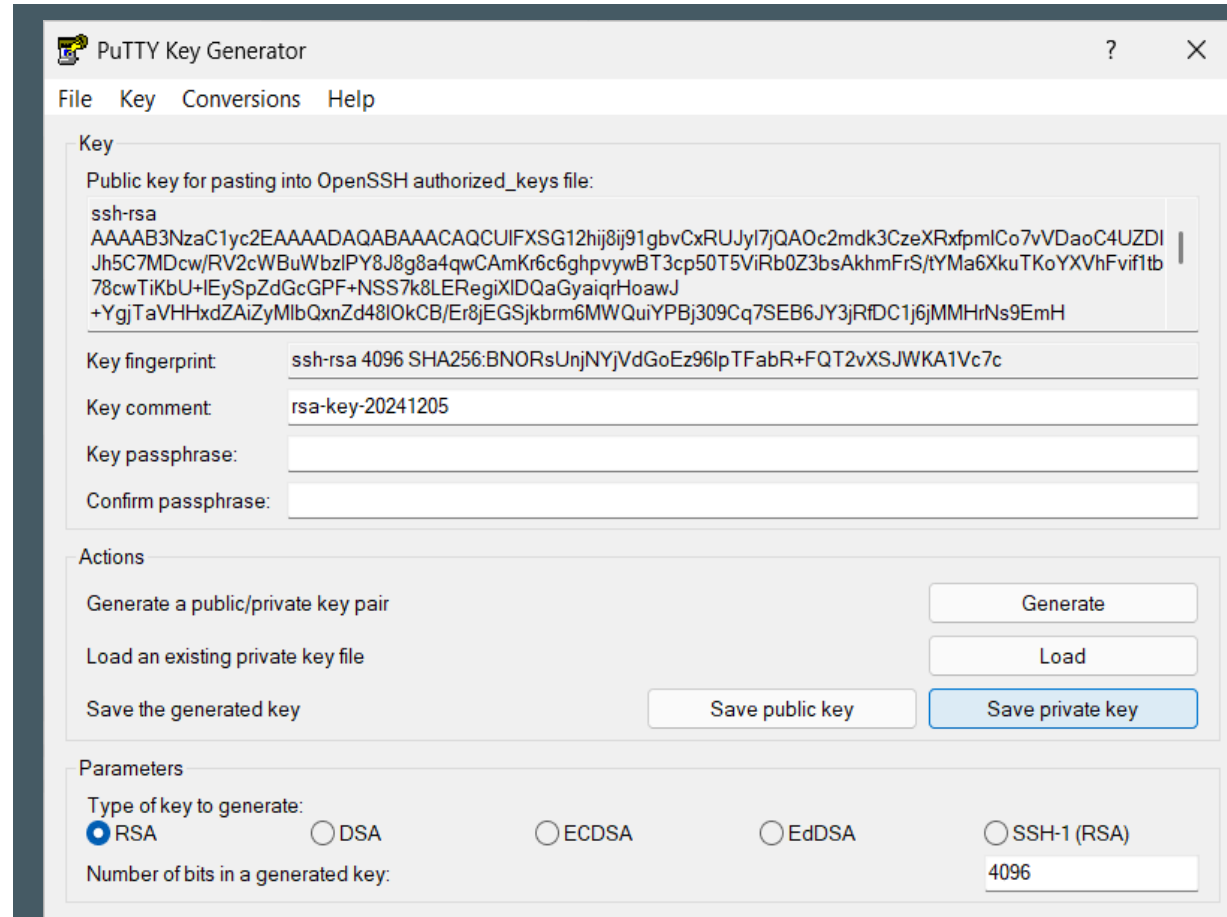
Type of key to generate:

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

Number of bits in a generated key:

Schlüsselpaar wurde erzeugt. Der öffentliche Schlüssel wird in der oberen Hälfte angezeigt.

Private Key speichern



PuTTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQCUiFXSG12hij8ij91gbvCxRUJyl7jQAOc2mdk3CzeXRxfpmlCo7vVDaoC4UZDI
Jh5C7MDcw/RV2cWBUWbzIPY8J8g8a4qwCAmKr6c6ghpvywBT3cp50T5ViRb0Z3bsAkHmFrS/tYMa6XkuTKoYXVhFvif1tb
78cwTiKbU+IEySpZdGcGPF+NSS7k8LERegiXIDQaGyaiqrHoawJ
+YgjTaVHHxdZAiZyMlbQxnZd48IOkCB/Er8jEGSjkbm6MWQuiYPBj309Cq7SEB6JY3jRfDC1j6jMMHrNs9EmH
```

Key fingerprint: ssh-rsa 4096 SHA256:BNORsUnjNYjVdGoEz96lpTFabR+FQT2vXSJWKA1Vc7c

Key comment: rsa-key-20241205

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

Parameters

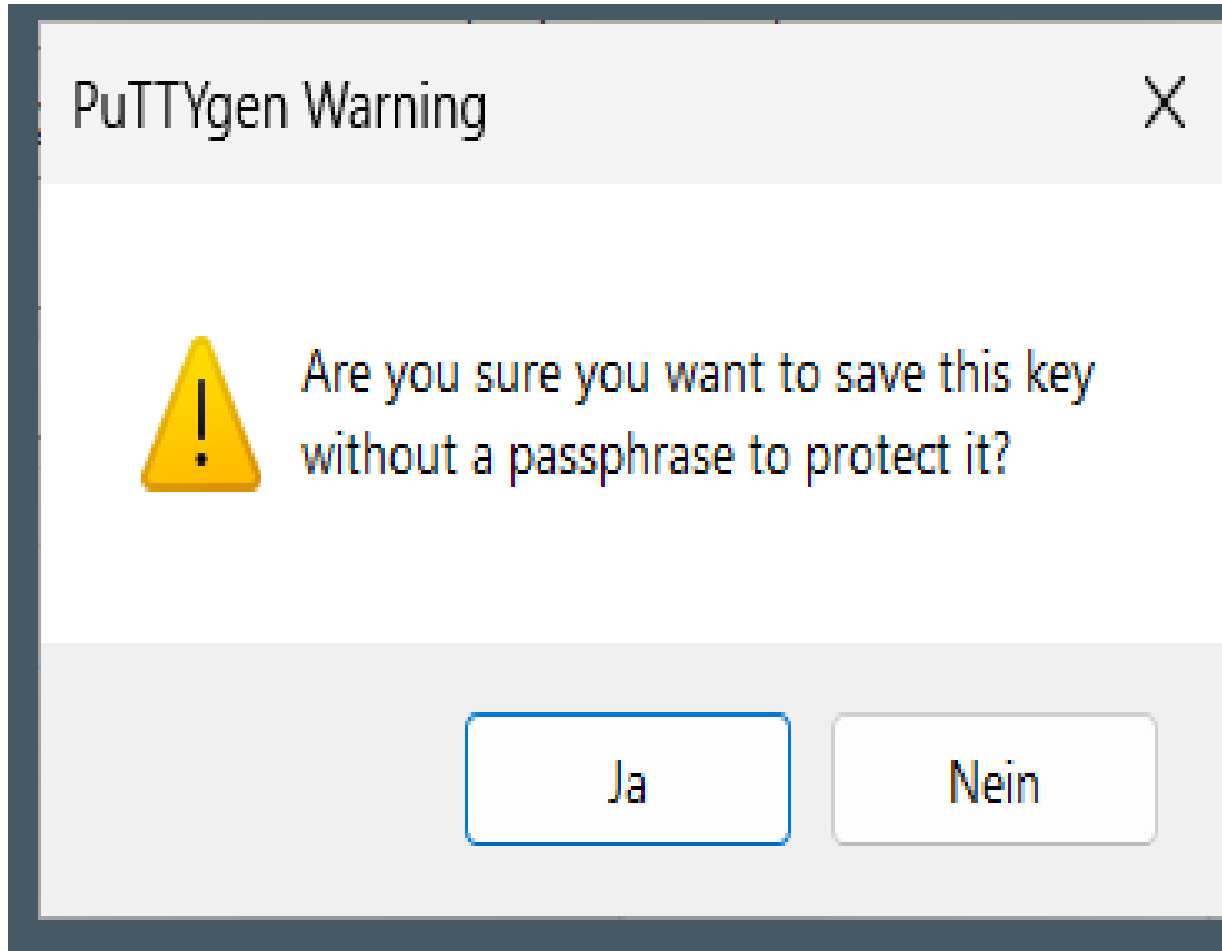
Type of key to generate:

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

Number of bits in a generated key: 4096

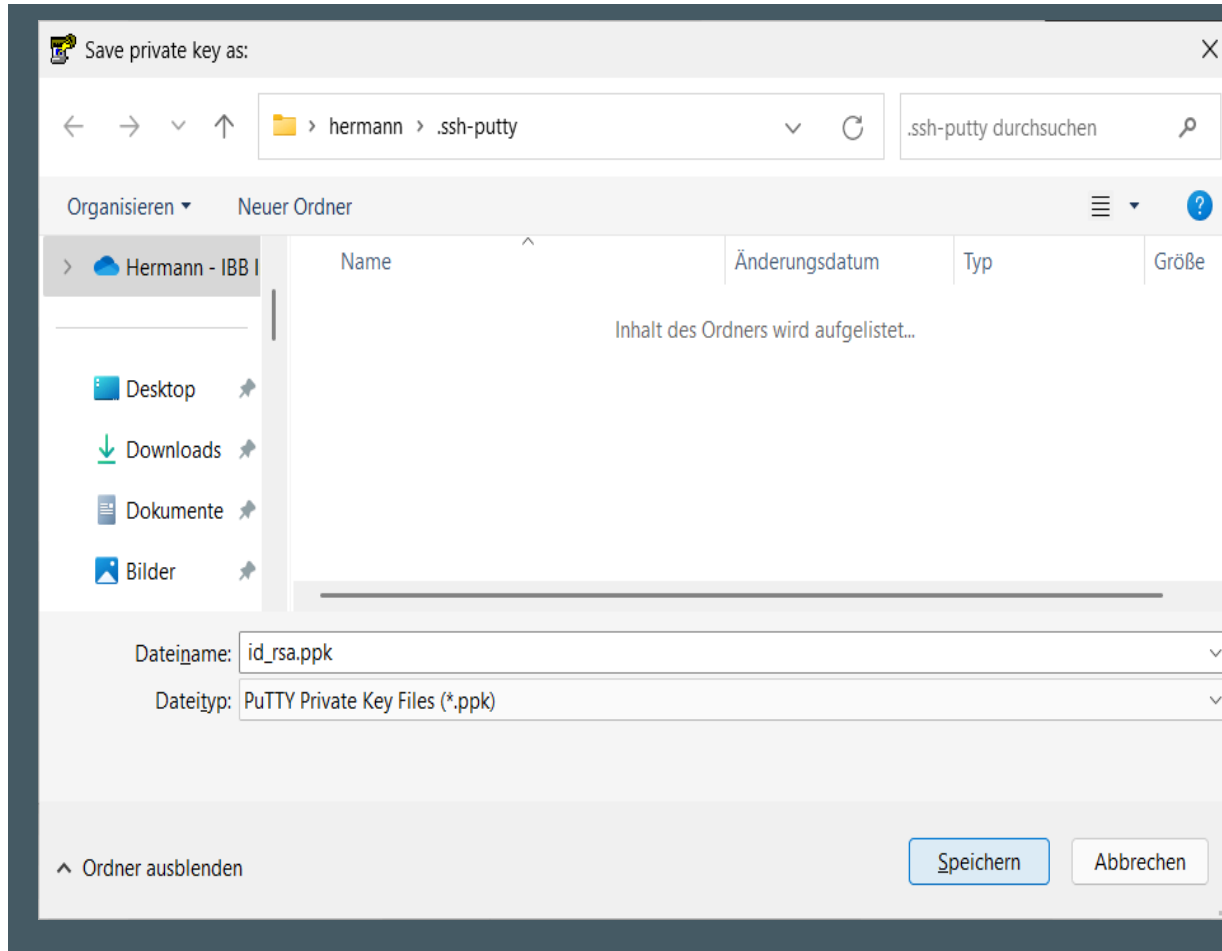
**Passphrase leer lassen, den
privaten Schlüssel
speichern**

Warnung bei leerer Passphrase



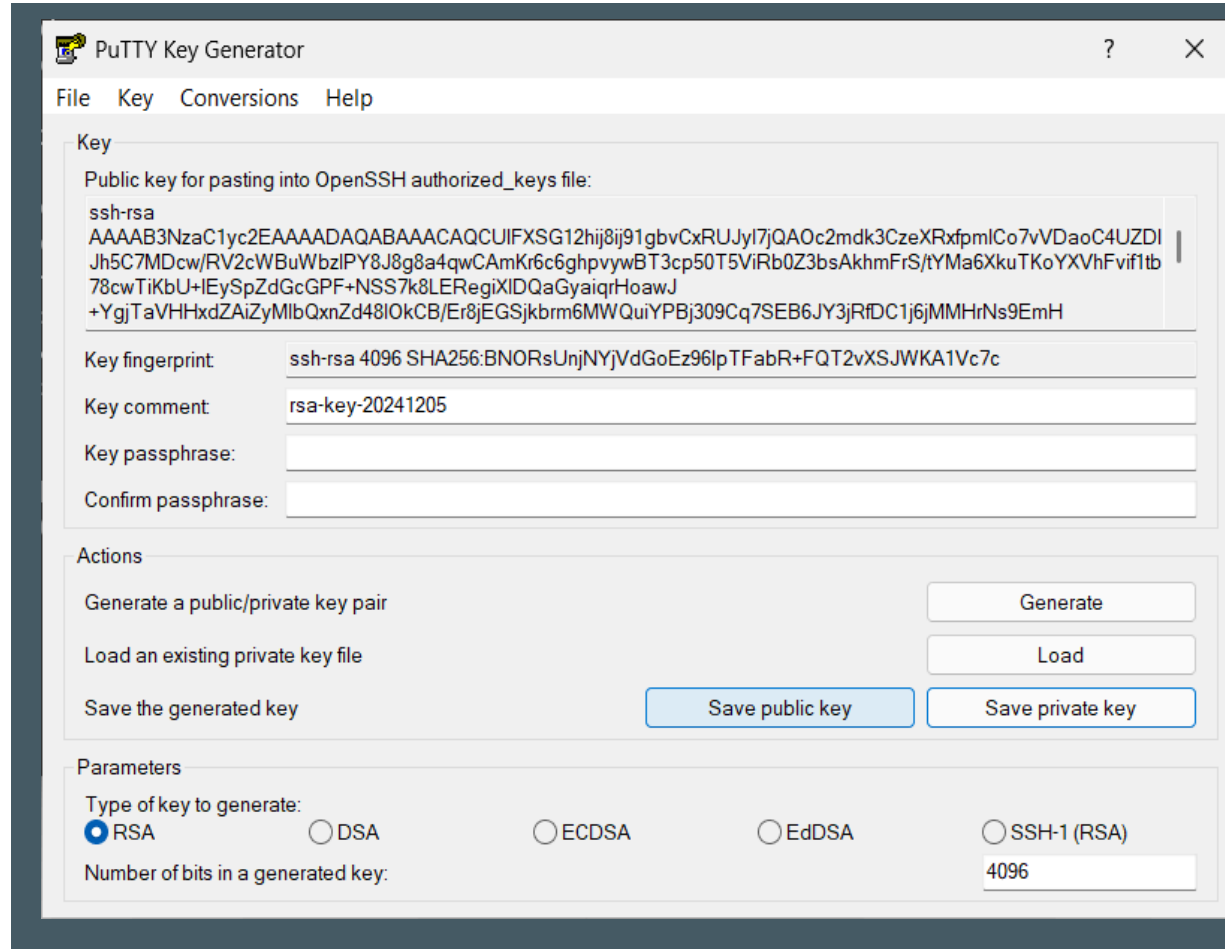
**Warnung, dass die
Passphrase leer gelassen
wurde**

Private Key: Speicherort und Dateiname



**Verzeichnis für die Ablage
des privaten Schlüssels und
Dateinamen wählen**

Public Key speichern



PuTTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQACUFXSG12hij8ij91gbvCxRUJyl7jQA0c2mdk3CzeXRxfpmlCo7vVDaoC4UZDI
Jh5C7MDcw/RV2cWBUWbzIPY8J8g8a4qwCAmKr6c6ghpvywBT3cp50T5ViRb0Z3bsAkHmFrS/tYMa6XkuTKoYXVhFvif1tb
78cwTiKbU+IEySpZdGcGPF+NSS7k8LERegiXIDQaGyaiqrHoawJ
+YgjTaVHHxdZaizyMlbQxnZd48IOkCB/Er8jEGSjkbm6MWQuiYPBj309Cq7SEB6JY3jRfDC1j6jMMHrNs9EmH
```

Key fingerprint: ssh-rsa 4096 SHA256:BNORsUnjNYjVdGoEz96lpTFabR+FQT2vXSJWKA1Vc7c

Key comment: rsa-key-20241205

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

Parameters

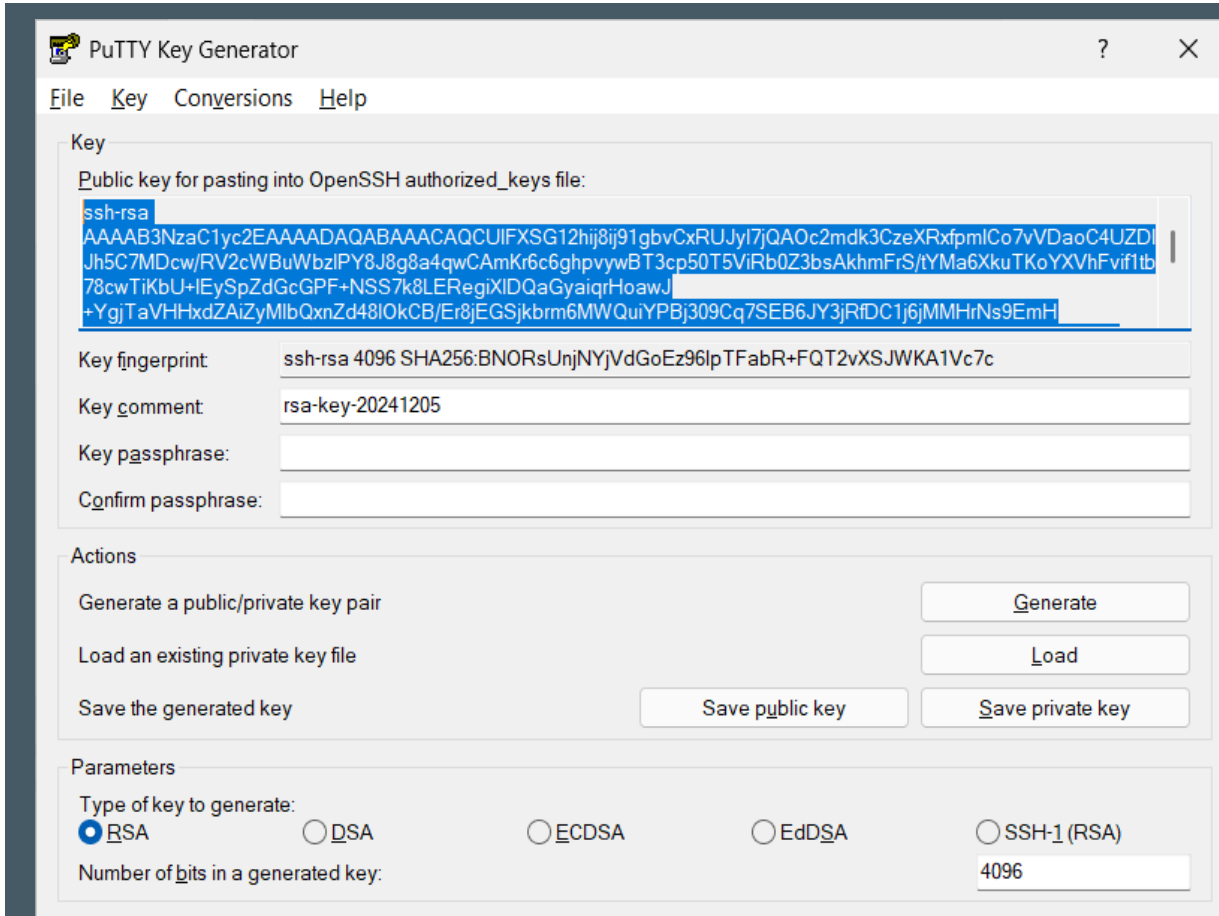
Type of key to generate:

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

Number of bits in a generated key: 4096

Öffentlichen Schlüssel
speichern

Public Key kopieren (zum Einfügen auf dem Remote Host)



The screenshot shows the PuTTY Key Generator window. The 'Key' section displays the public key for pasting into the OpenSSH authorized_keys file. The key is highlighted in blue. Below the key, the key fingerprint and comment are shown. The 'Actions' section has buttons for 'Generate', 'Load', 'Save public key', and 'Save private key'. The 'Parameters' section shows the key type as RSA and the number of bits as 4096.

PuTTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQACUJFSG12hij8ij91gbvCxRUJyl7jQAoc2mdk3CzeXRxfpmlCo7vVDaoC4UZDI
Jh5C7MDcw/RV2cWBUWbzIPY8J8g8a4qwCAmKr6c6ghpvywBT3cp50T5ViRb0Z3bsAkhmFrS/tYMa6XkuTKoYXVhFvif1tb
78cwTiKbU+IEySpZdGcGPF+NSS7k8LERegIXIDQaGyaiqrHoawJ
+YgjTaVHhxdZAIzYmIbQxnZd48IOkCB/Er8jEGSjkbm6MWQuiYPBj309Cq7SEB6JY3jRfDC1j6jMMHrNs9EmH
```

Key fingerprint: ssh-rsa 4096 SHA256:BNORsUnjNYjVdGoEz96lpTFabR+FQT2vXSJWKA1Vc7c

Key comment: rsa-key-20241205

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

Parameters

Type of key to generate:

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

Number of bits in a generated key: 4096

**Den öffentlichen Schlüssel
markieren und kopieren**

Remote Host: Public Key bekannt machen

Der zuvor in PuTTYGen kopierte öffentliche Schlüssel wird in die Datei `~/.ssh/authorized_keys` auf dem entfernten Host eingefügt.

- Dazu wird eine `ssh`-Sitzung zum entfernten Host mit Passwort-Login aufgebaut.
- Ein Editor wird gestartet und der kopierte öffentliche Schlüssel wird in `~/.ssh/authorized_keys` eingefügt.
- Datei speichern, Editor beenden und die `ssh`-Sitzung beenden.

Passwort-Anmeldung und Editor starten

```
hermann@deb-srv: ~  
Using username "hermann".  
hermann@deb-srv.mshome.net's password:  
Linux deb-srv 6.1.0-28-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.119-1 (2024-11-22)  
) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Wed Dec 4 21:43:30 2024 from 172.29.144.1  
hermann@deb-srv:~$ vi .ssh/authorized_keys
```

**Anmeldung auf dem
Remote Host mit Passwort
und einen Editor (`nano` oder
`vi`, , hier: `vi`) starten**

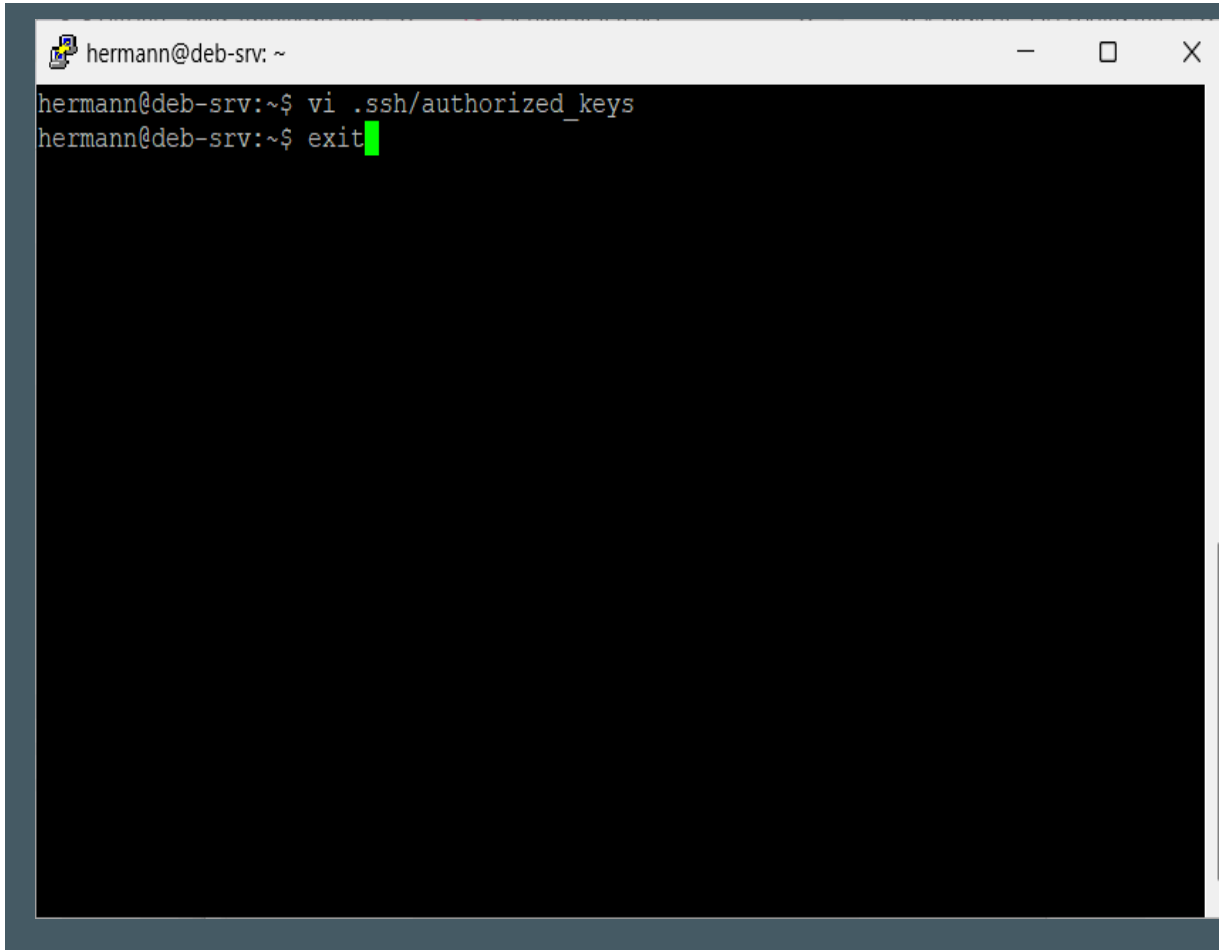
Public Key ans Ende von `~/.ssh/authorized_keys`

```
hermann@deb-srv: ~  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQC3yJ/tPz4XTqS9axj+QqNN85+x+vQ6M6mKGx9X9WAXyC  
zYRLXCFT1vs00YhIaghrFkzMMwYHPJJZFYlws2b5VIb4mmpR7pBAI41Y3Na9vBxThv9jIMbyHaYasvf+ol  
eTyCvDPTMg8g7UiWk/BInp7oc4mIi+bTEcu+XStfJq4BEvzYWynnEJPG4ViwcdMWjhtjlvz5cNssWgZoE  
InEXd2UbQOPSec4GwG3pyGvuPBa5xmcXeq0uK0AWNvNiOqVtONDvfPdtXERoz4VTiuvog1comV6aW4yPEO  
U0dfwTRKSpMj172vFshTg0446rYeXziGWM78FkOYzfDkL9wQdxRa1QaD7ERIwSilhIoo3Im7j00c2yIWzX  
BDUK4Jvp40Z0gT3jlZXZhTHOlGEb94dI5H28CU/10leOs1+CLVpxMjLeeaenRmnpB5nS7cvZ8sTkqVztMO  
GfR9nJNX3Lh+tIoCPmhPt+NzVfAT+wHj+wQRRD6vj9E8sq+PzqAr2PoDe8ZgQMdo2CeVy407DFmb/GhtHs  
Ob789VInyrxe7p2T1nFI+v2snXUOE02wwBc5AVyfe9wnG5dMoNN/8DLfGdR1qCubAlje/AqRSYxnFsH7R  
8VUrp6vT0yMRUk1vT10VJyYrmPpfdzJ0tLbtj5DJerN2JBBpvHLdM2mmHEc0TNC9IQ== hermann@tuxpl  
4-win11^M  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQCUIFXSG12hij8ij91gbvCxRUJyl7jQAoc2mdk3CzeXRr  
fpm1Co7vVDaoC4UZDlJh5C7MDcw/RV2cWBUwbzIPY8J8g8a4qwCAmKr6c6ghpvywBT3cp50T5ViRb0Z3bs  
AkhmFrS/tYMa6XkuTKoYXVhFvif1tb78cwTiKbU+1EySpZdGcGPF+NSS7k8LERegiXIDQaGyaiqrHoawJ+  
YgjTaVHHxdZAIzYmIbQxnZd48IOkCB/Er8jEGSjkbrm6MWQuiYPBj309Cq7SEB6JY3jRfDC1j6jMMHrNs9  
EmH+1Xh49cX0+/xAsv6pdBKRbLEyaMwCA5kci+8RZGrubTeOkQx6LX1ICqTl/1PrnlFRKV8EzsaConmHiE  
PFyDQI4o7UYvR+pa+wiINTuKYqyYLMnKuLH5bxGcKT2yqMiMeHLDSKTT7VcAA3aKIXOfp6EOOUL+M1wKZk  
gm1wIP43z5/hb4S2bFnFIHr+ph0vrL154Tqs9qAtMglAgdpU8L1fb84oCGkr4LbmdxObr9UzSzl90a8BVf  
I63b+lhvTDwr6Kte4bsJc0rEFiPeLlaogtDFmSf5JtNtail++heMQate4XwYNPPHSTRRa50UyfZf/3xIKk  
2hSr72+lgef0w8GrwFmYHkm8oL0IezzZ6GvOxOotlhogu2B4lN228Pz1R33Ri6xtpw== rsa-key-20241  
205  
~  
~  
~
```

**Öffentlichen Schlüssel am
Ende der Datei**

**`~/.ssh/authorized_keys`
einfügen**

Speichern und Sitzung beenden



```
hermann@deb-srv: ~  
hermann@deb-srv:~$ vi .ssh/authorized_keys  
hermann@deb-srv:~$ exit
```

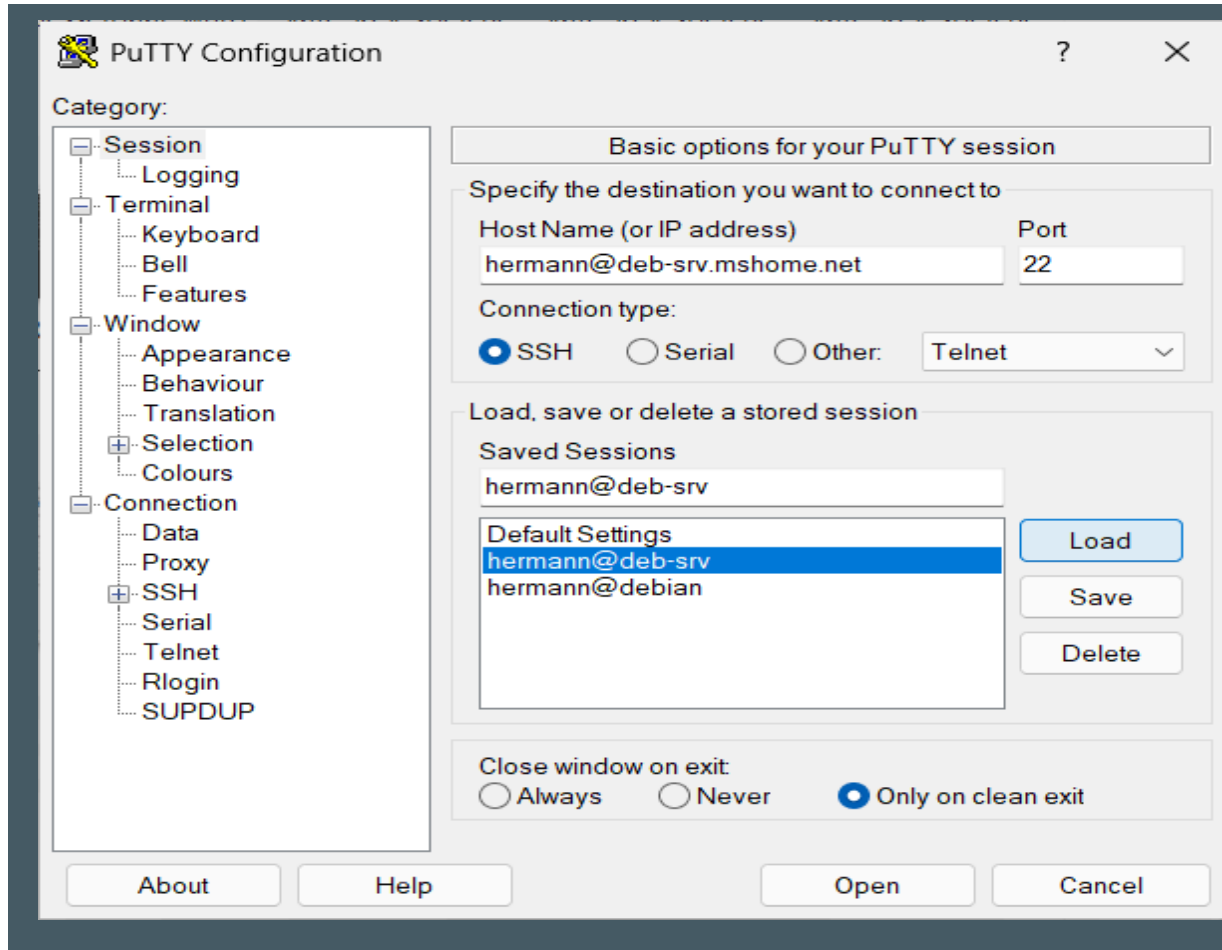
`.ssh/authorized_keys`
**speichern, Editor verlassen
und Sitzung beenden**

PuTTY: Private Key bekannt machen

Nach dem der public Key auf dem entfernten Linux-Host eingetragen wurde, muss der gespeicherte private Key in PuTTY als Authentifizierungsmethode konfiguriert werden, damit das key-basierte, passwortlose Login funktioniert. Dazu wird in PuTTY

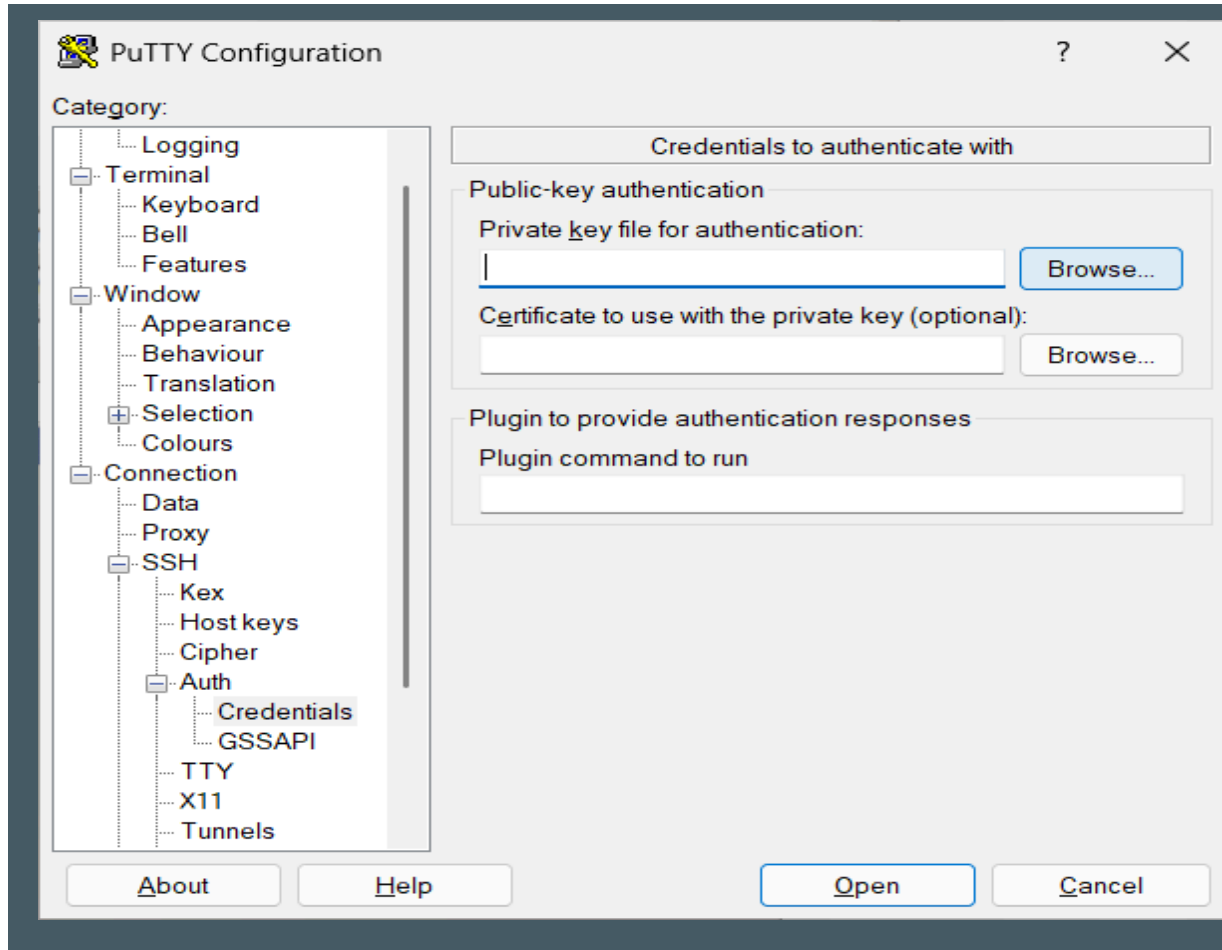
- die betreffende `ssh`-Sitzung geladen,
- der zuvor gespeicherte private Key ausgewählt und
- die geänderte Sitzungs-Konfiguration gespeichert.
- Nun kann die `ssh`-Verbindung zum entfernten Host ohne Passwort aufgebaut werden.

ssh-Sitzung laden



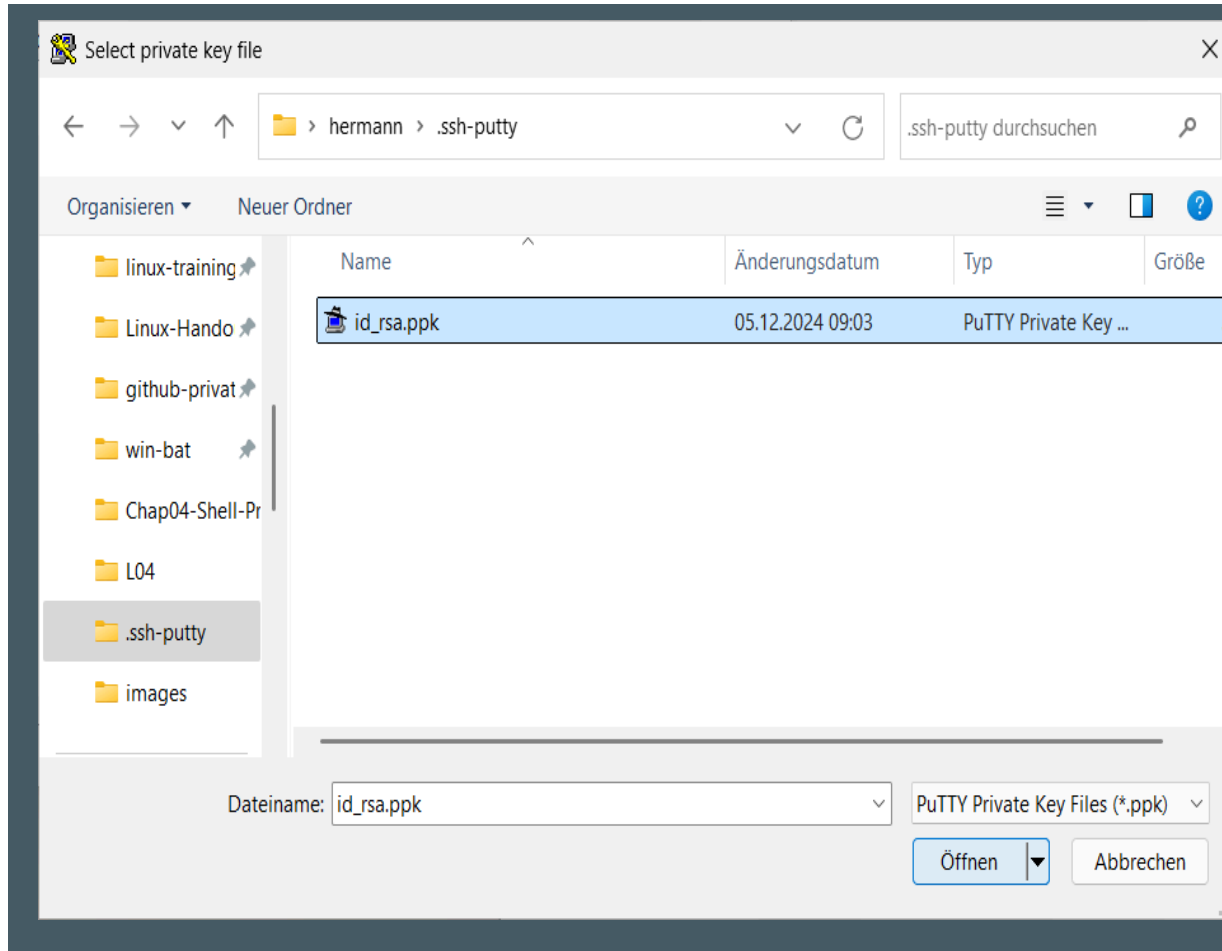
Die gewünschte **ssh** -
Sitzung wird geladen (hier:
deb-srv)

Zu **ssh**-Credentials navigieren



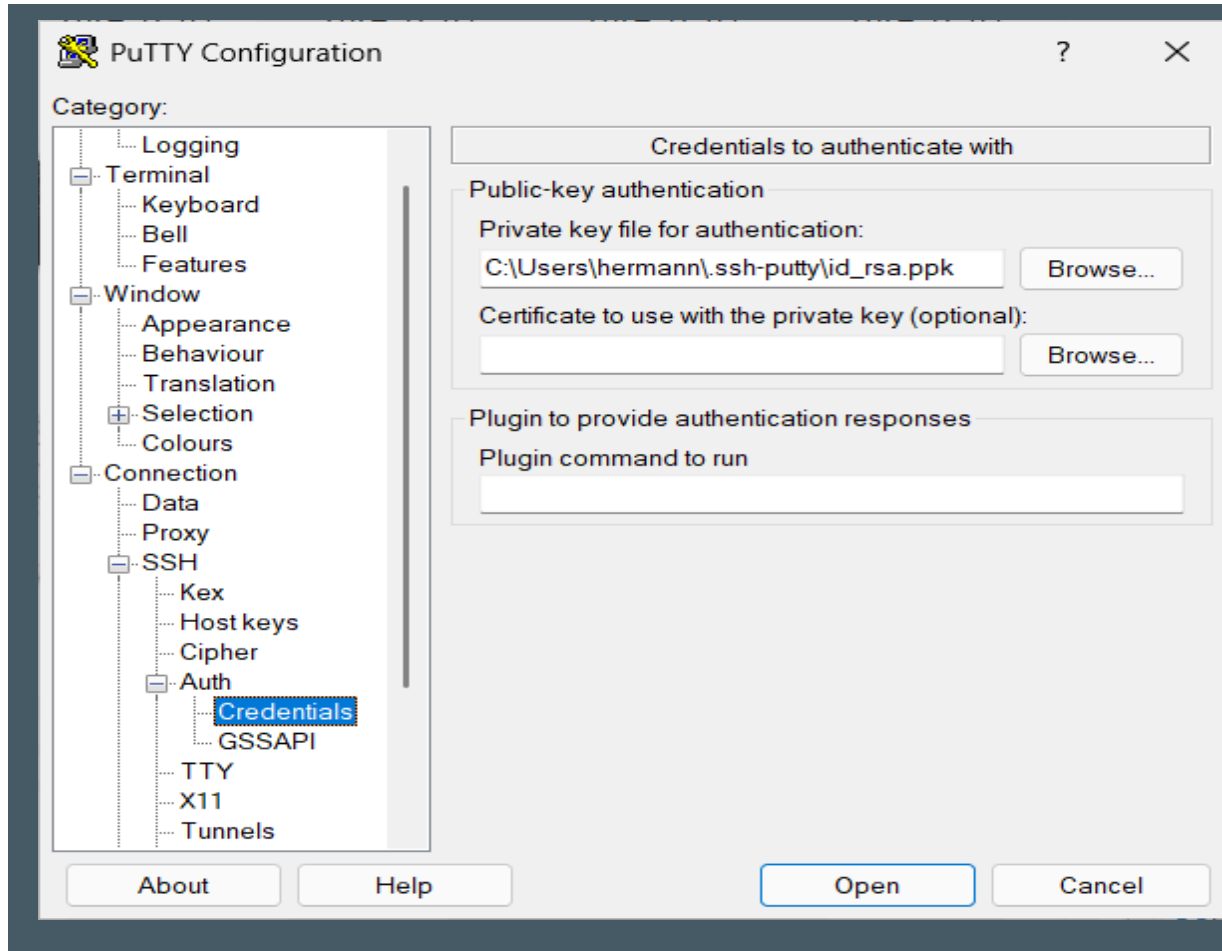
**Im linken Fenster auf
"Connection" -> "SSH" ->
"Auth" -> "Credentials"
klicken. Rechts ist ein Feld
mit der Bezeichnung
"Private key file for
authentication" zu sehen.
Hier auf "Browse" klicken**

Private Key File auswählen



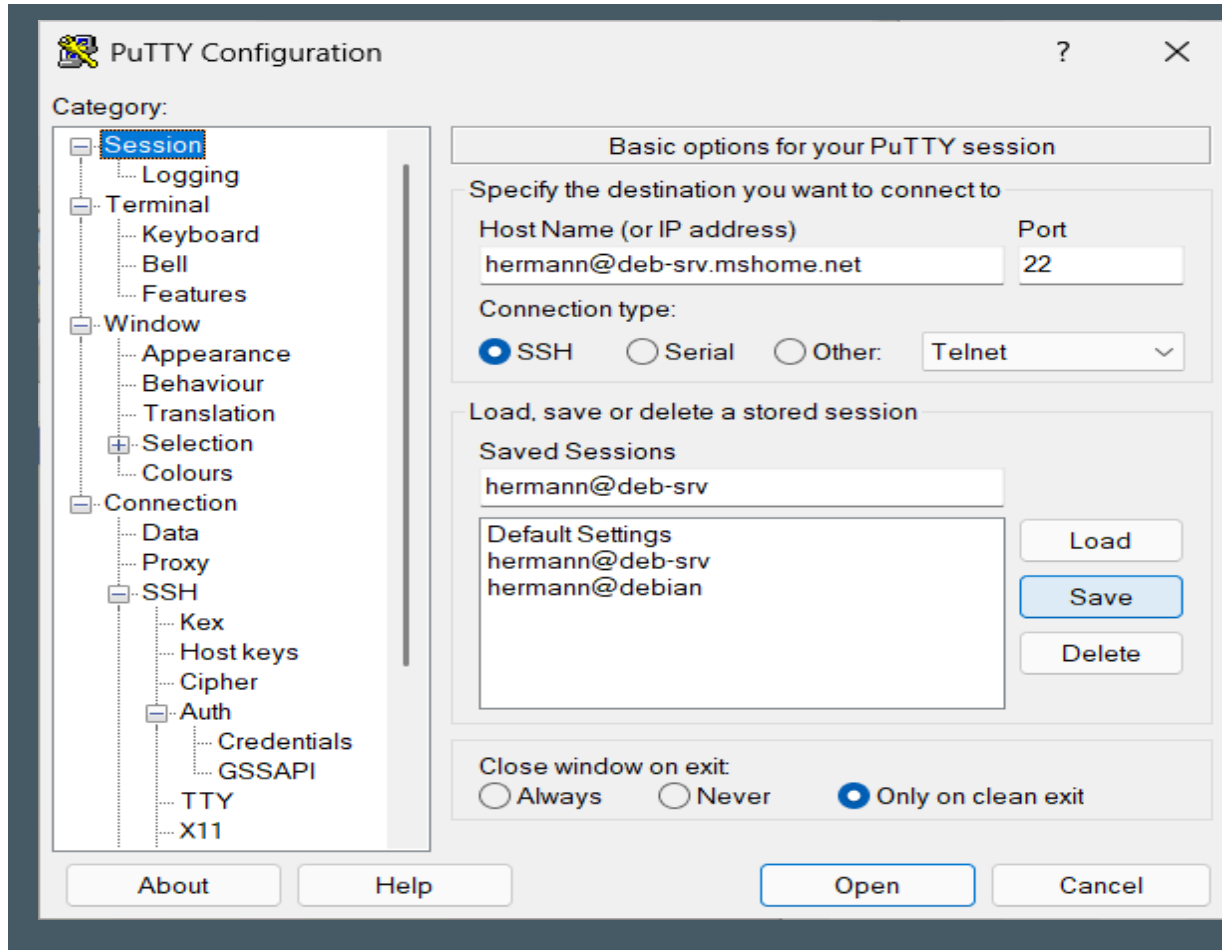
**Das zuvor in PuTTYGen
gespeicherte private key
file wird ausgewählt.**

Private Key File ausgewählt



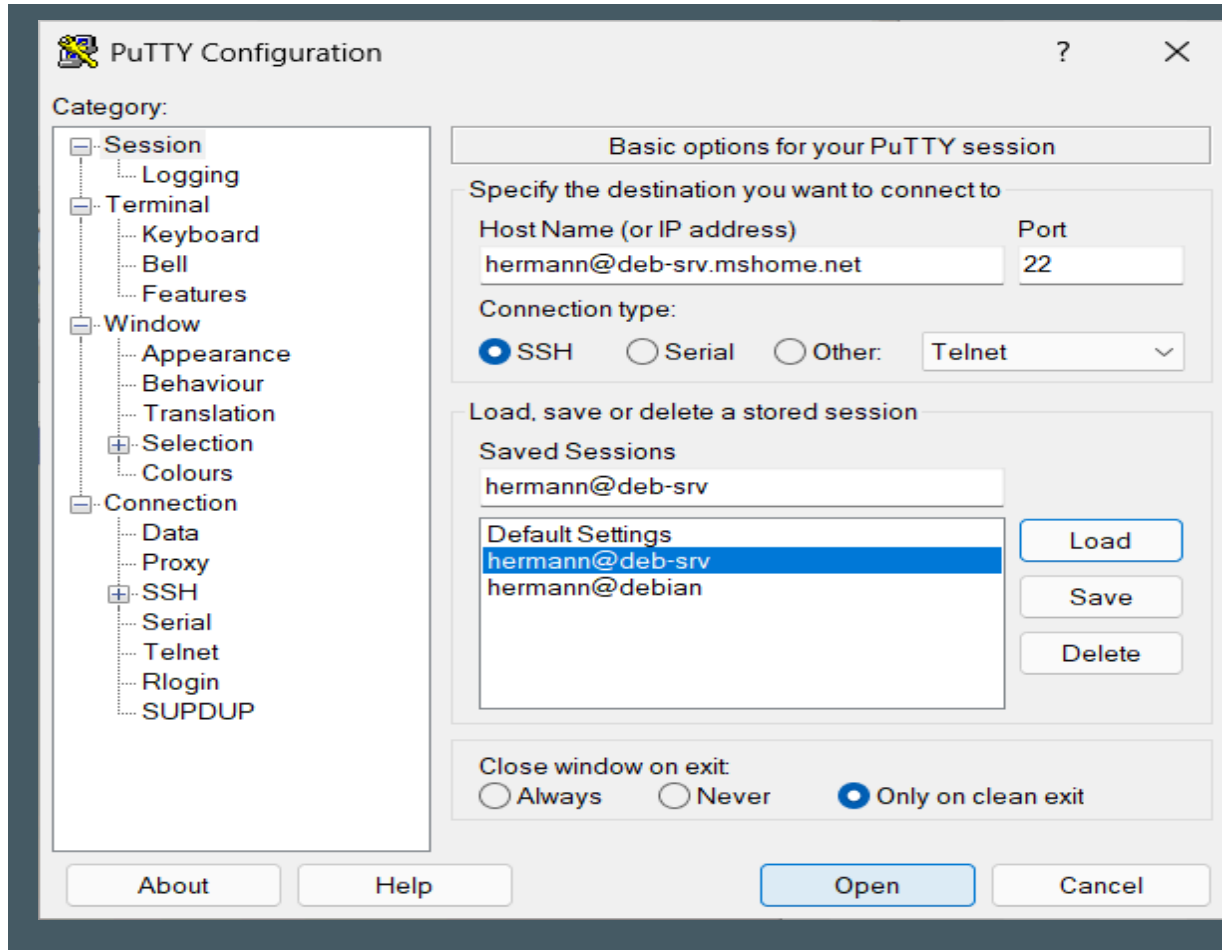
**Pfad des ausgewählten
private key file ist nun
eingetragen.**

ssh -Sitzungs-Konfiguration speichern



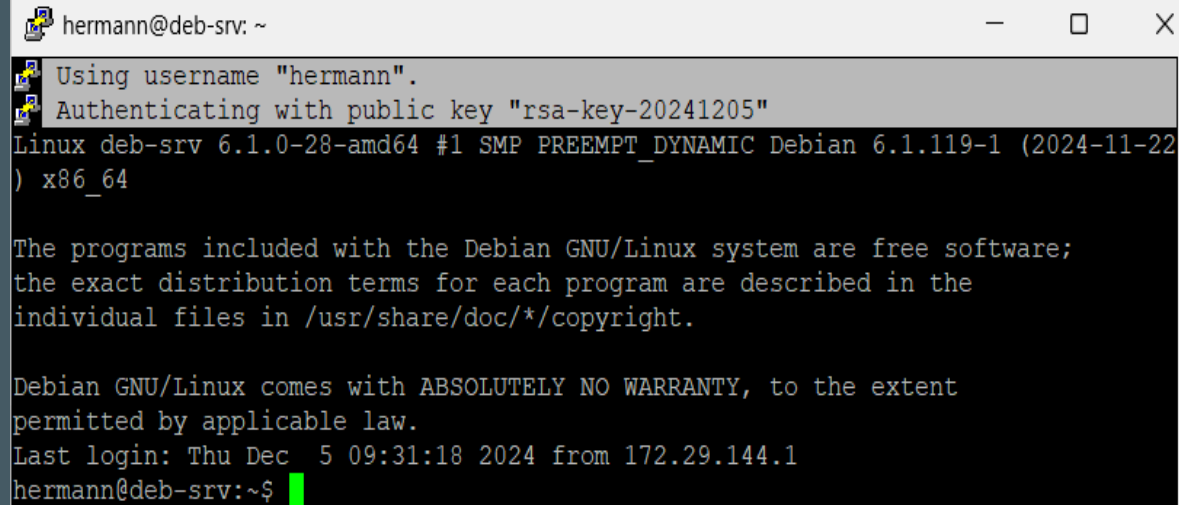
Im linken Fenster ganz oben auf "Session" klicken und die geänderte Sitzungskonfiguration im rechten Fenster mit "Save" speichern.

ssh -Sitzung öffnen



Mit dem Klick auf "Open" wird die `ssh`-Verbindung zum entfernten Host aufgebaut.

ssh-Sitzung ohne Passwortabfrage



A terminal window titled 'hermann@deb-srv: ~' showing an SSH session. The window has standard Linux window controls (minimize, maximize, close). The terminal output is as follows:

```
hermann@deb-srv: ~  
Using username "hermann".  
Authenticating with public key "rsa-key-20241205"  
Linux deb-srv 6.1.0-28-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.119-1 (2024-11-22)  
) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Thu Dec  5 09:31:18 2024 from 172.29.144.1  
hermann@deb-srv:~$
```

**Man ist ohne
Passwortabfrage auf dem
entfernten Host eingeloggt.**

Links

- <https://www.howtoforge.de/anleitung/key-basierte-ssh-logins-mit-putty/> - Auf dieser Seite ist eine sehr ausführliche Anleitung für das key-basierte Login mit PuTTY zu finden. Allerdings wird dort die Passphrase nicht leer gelassen. Dann würde man zwar nicht nach dem Passwort gefragt, aber die Passphrase müsste bei jedem Login eingegeben werden. Mit dem Tool **Pageant** kann man die Passphrase einmalig eingeben und sie wird dann für die Dauer der Windows-Sitzung gespeichert.