

# PuTTYgen

## Generation of SSH-Key

### Generation of SSH-Key using PuTTYgen

Autor: AZI  
Date: 20.08.2008

- 1 INTRODUCTION..... 2**
- 2 INSTALLATION ..... 2**
- 3 GENERATE A SSH2 DSA PUBLIC KEY ..... 2**
  - 3.1 FIRST APPEARANCE ..... 2
  - 3.2 CONFIGURATION ..... 2
  - 3.3 GENERATE KEY ..... 3
- 4 COPY KEY TO DEVICE ..... 5**
- 5 SAVE KEY TO LOCAL COMPUTER ..... 5**
- 6 CONFIGURE PUTTY TO USE SSH ..... 5**
  - 6.1 SESSION SETTINGS ..... 5
  - 6.2 TERMINAL SETTINGS ..... 6
  - 6.3 CONNECTION SETTINGS..... 7
  - 6.4 SSH SETTINGS ..... 8
  - 6.5 OPEN THE SESSION WITH SSH..... 9
- 7 FURTHER HELP ..... 10**

# PuTTYgen

## Generation of SSH-Key

### 1 Introduction

Steps for proper configuration and use of PuTTYgen to generate an SSHv2 public key.

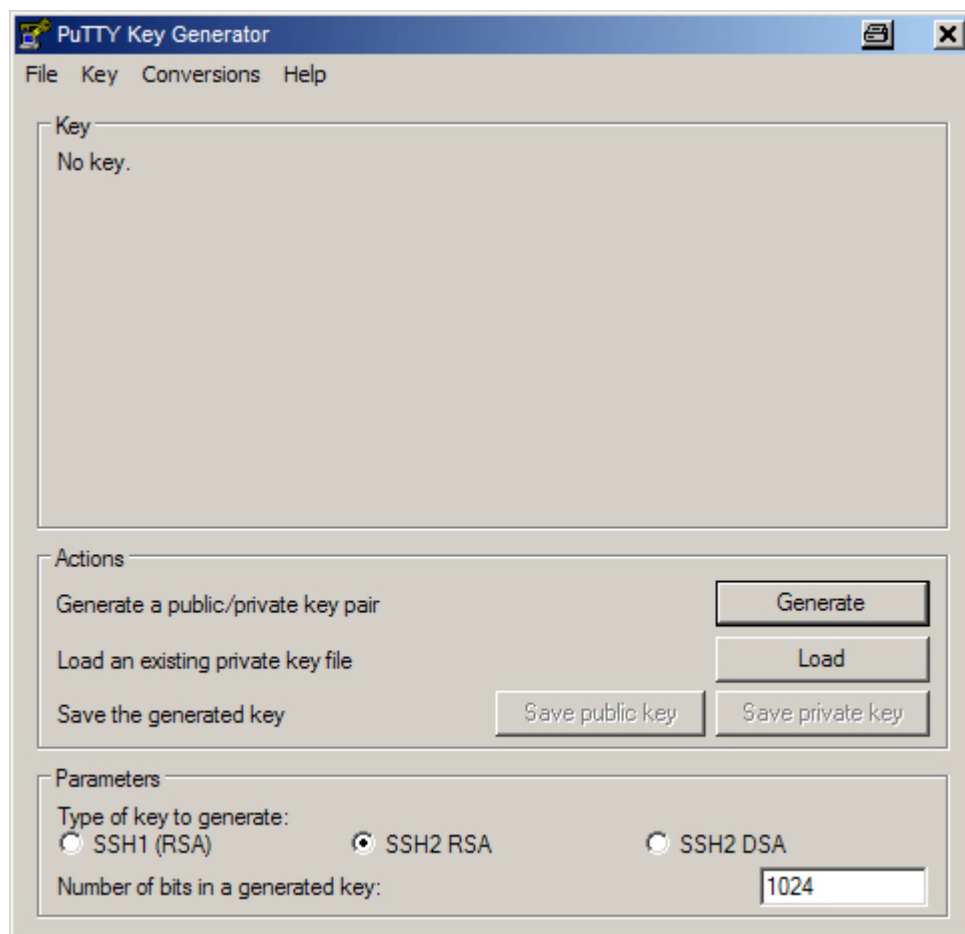
### 2 Installation

Copy the puttygen.exe file to your computer. No extra installation work is necessary.

### 3 Generate a SSH2 DSA public key

#### 3.1 First Appearance

After start of PuTTYgen the following window will open:



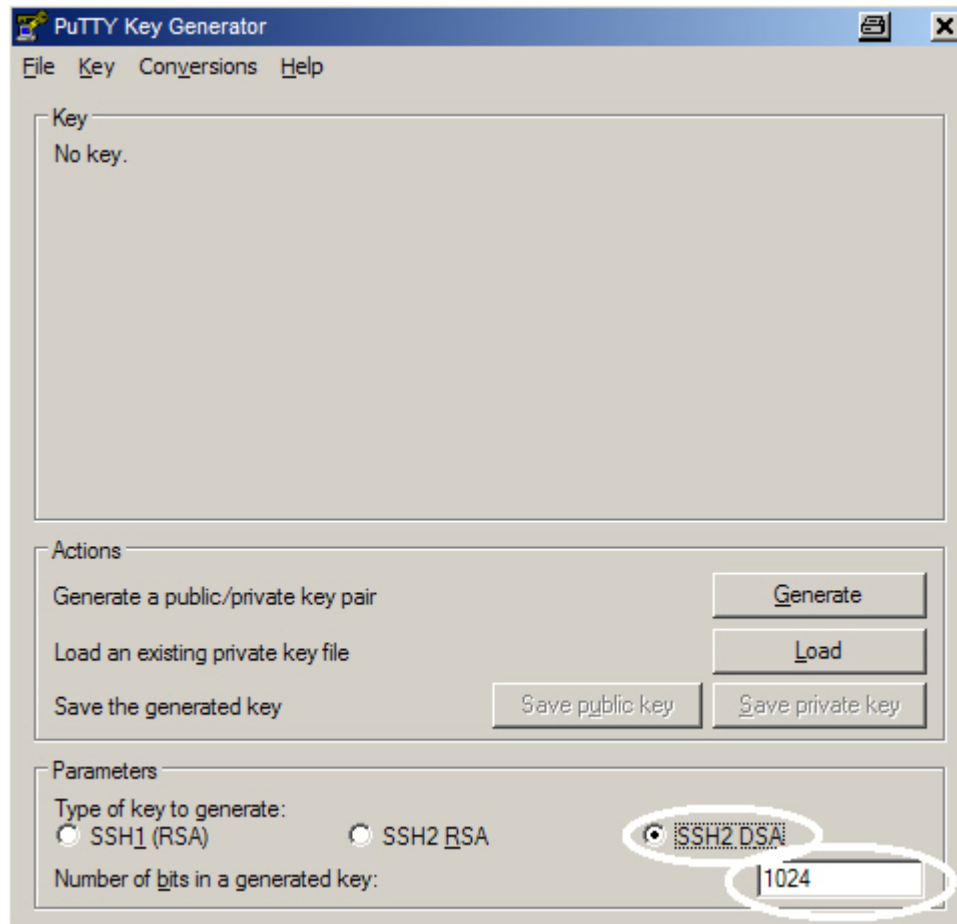
#### 3.2 Configuration

Use the following settings:

# PuTTYgen

## Generation of SSH-Key

- type of key to generate: SSH2 DSA
- Number of bits in a generated key: 1024



### 3.3 Generate Key

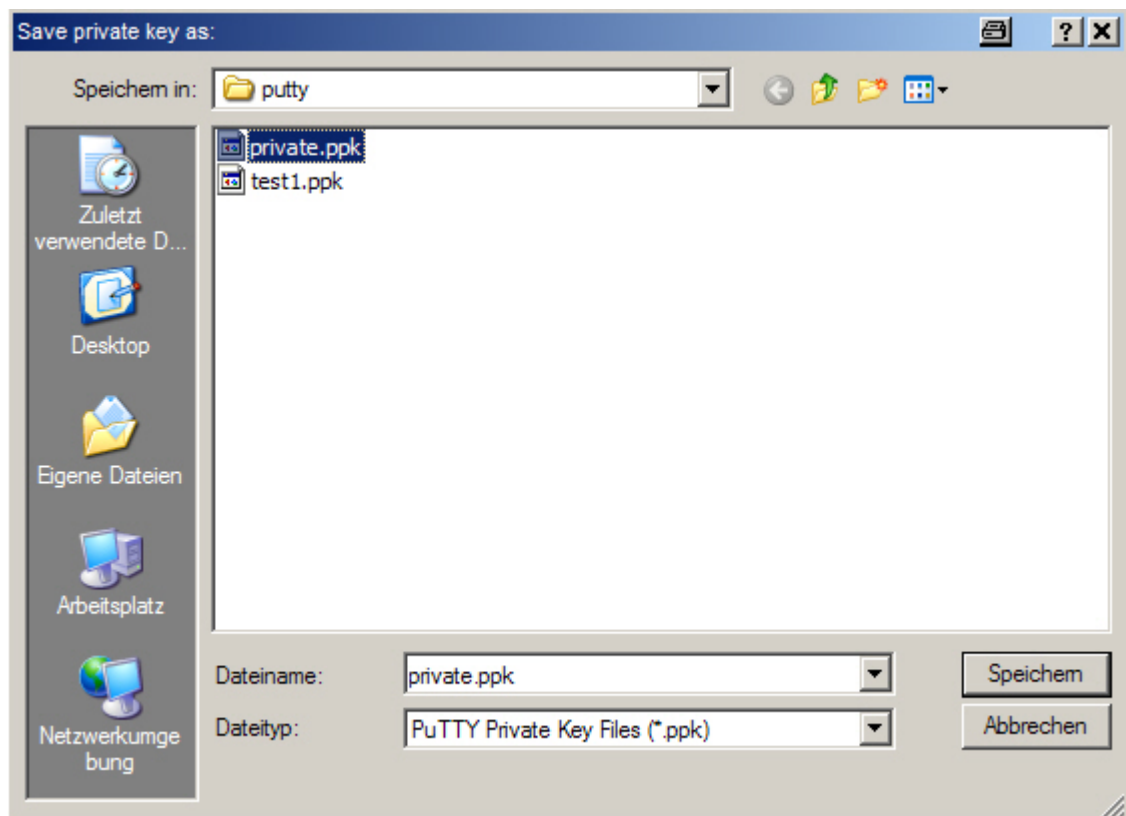
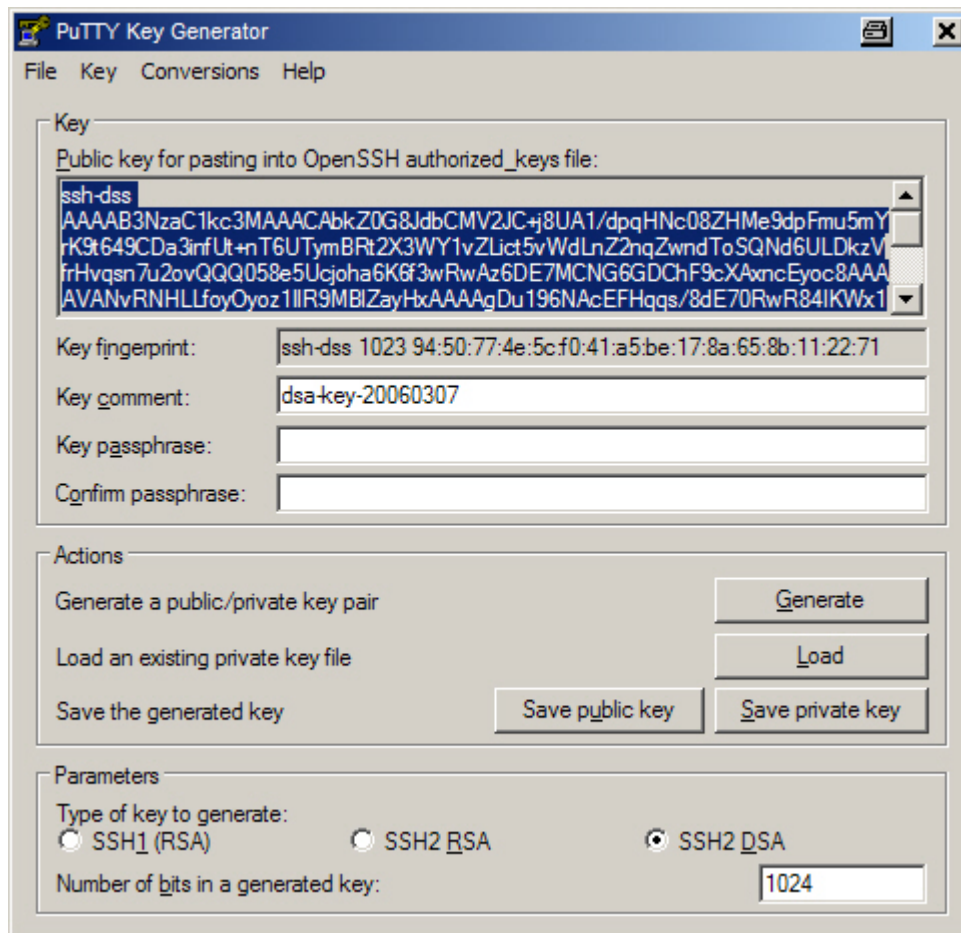
Press the "Generate" Button.

PS: Do not forget to move the mouse – this will speed up the generation!!

The openssh public key appears under the line:  
"Public key for pasting into OpenSSH authorized keys file"  
It look something like this:

# PuTTYgen

## Generation of SSH-Key



## PuTTYgen

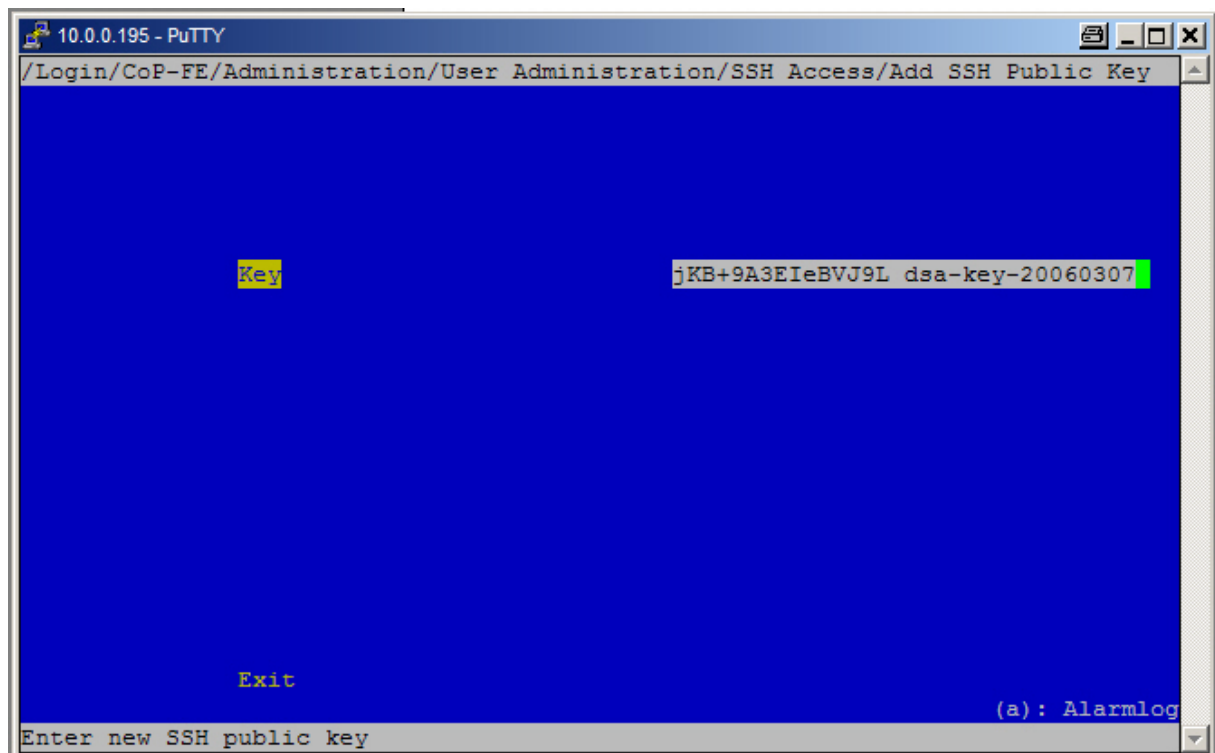
### Generation of SSH-Key

#### 4 Copy key to device

After the public key is generated, it has to be copied to the device (e.g. EDX1000).  
Enter the Administration menu and navigate to User Administration -> SSH Access -> Add key.

Select "Key" and press Enter. Copy the complete key (starting with "ssh-dss AAAAB3...dsa-key-date") into the field. Use CTRL+INS for Copy and SH+INS for Paste.

Press Enter again, to make the key available to the device.



#### 5 Save key to local computer

Store the generated key to your local computer, to make it usable for further operations.  
Press "Store private key".

Press "Yes" in the window "Are you sure you want to save this key without a passphrase to protect it?"

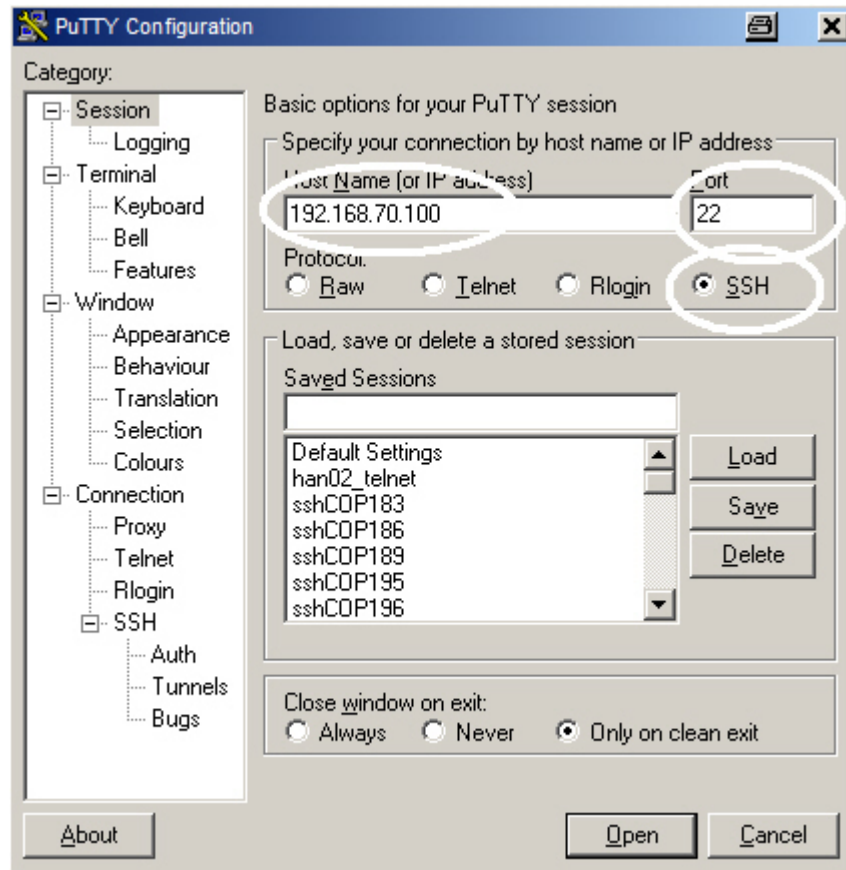
#### 6 Configure PuTTY to use SSH

##### 6.1 Session Settings

# PuTTYgen

## Generation of SSH-Key

Enter in the session menu the IP address of the device and select SSH protocol. Port 22 is the default for SSH and is chosen automatically.

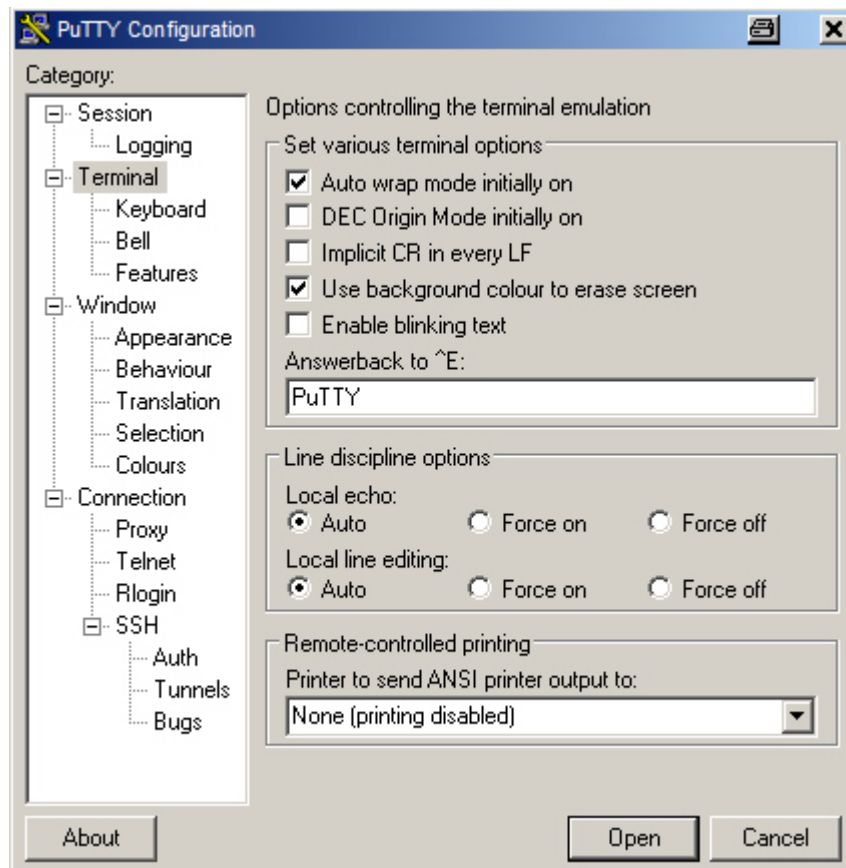


## 6.2 Terminal Settings

Configure the terminal to erase everything, when the connection is started:

# PuTTYgen

## Generation of SSH-Key



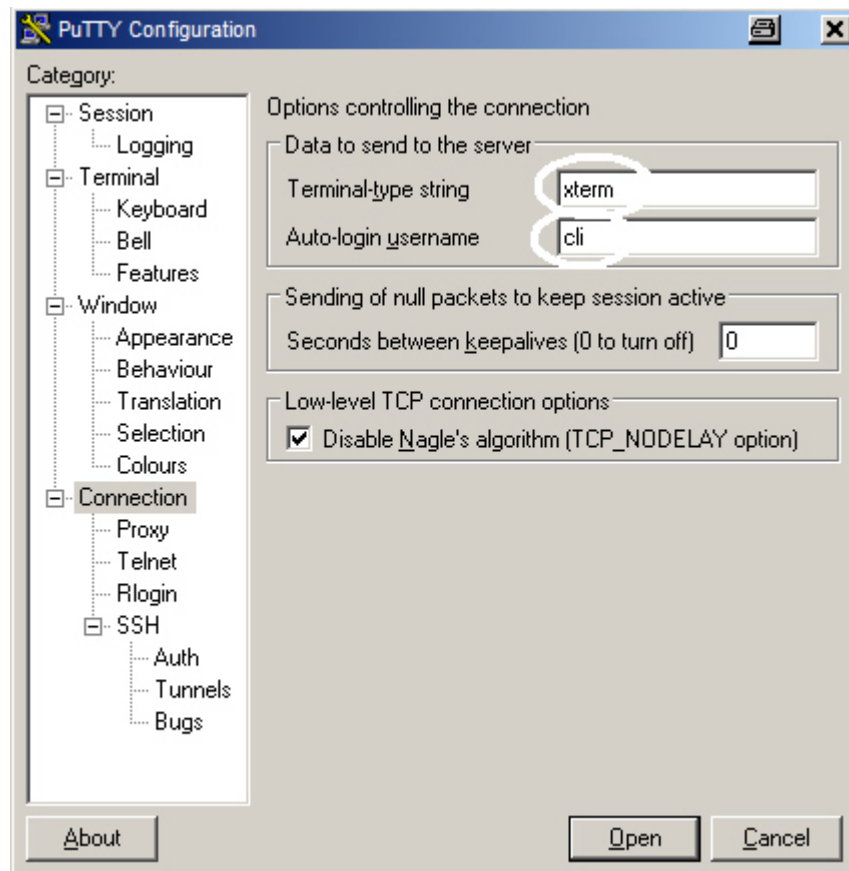
### 6.3 Connection Settings

Configure the SSH session to use xterm as terminal type and the user "cli" as user-ID for auto-login.

Remark: User "cli" is a predefined LINUX user on the device and it must not be defined in the administration menu. Use always user "cli"!

# PuTTYgen

## Generation of SSH-Key



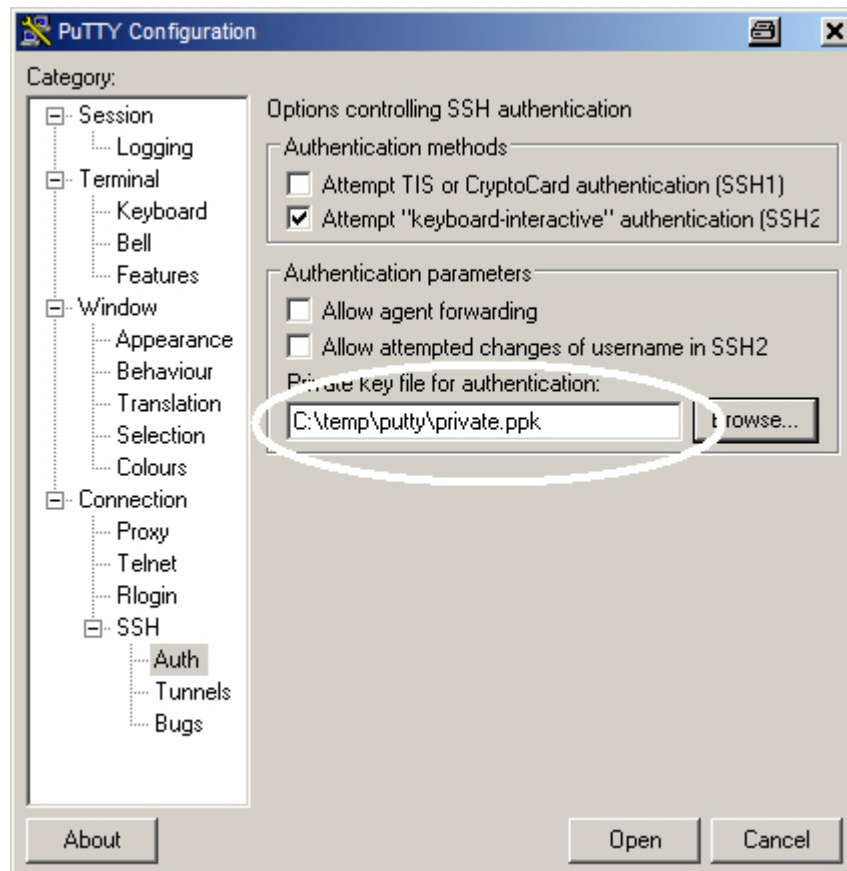
### 6.4 SSH Settings

Select preferred protocol = SSH version 2,  
Enter the file name of the previous stored private SSH key on your computer in the "Auth" –  
Menu:



# PuTTYgen

## Generation of SSH-Key

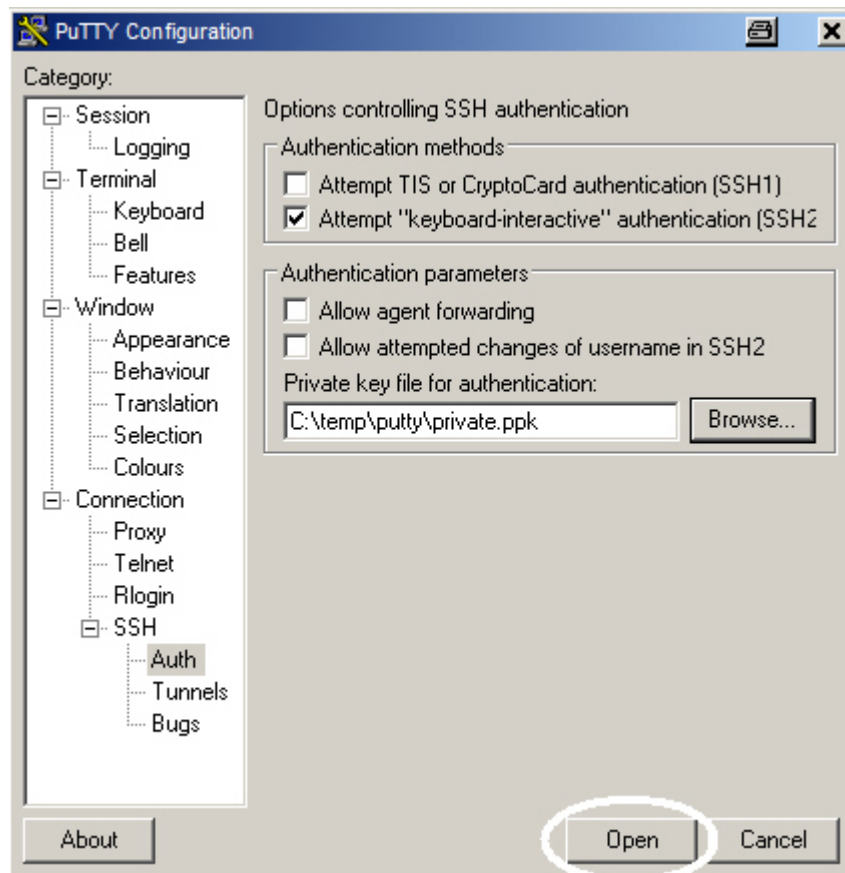


### 6.5 Open the session with SSH

Press "Open" to start the session. The keys are checked and the "normal" CLI window appears to log you into the system.

# PuTTYgen

## Generation of SSH-Key



## 7 Further help

For further help, please contact arcutronix GmbH at

[service@arcutronix.com](mailto:service@arcutronix.com) or meet us at the Internet

[www.arcutronix.com](http://www.arcutronix.com)