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 GENERALE REY | |
| 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 |
| 6.5 OPEN THE SESSION WITH SSH | 8 Q |
| | 10 |

arcutronix

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:

| PuTTY Key Generator | | 😑 🔀 |
|---|-----------------|------------------|
| File Key Conversions Help Key No key. | | |
| | | |
| Actions | | |
| Load an existing private key file | | Load |
| Save the generated key | Save public key | Save private key |
| Parameters | | |
| Type of key to generate: C SSH1 (RSA) © SSH2 RSA | O SSI | H2 DSA |
| Number of bits in a generated key: | | 1024 |

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

| PuTTY Key Generator | | <u>a</u> × |
|---|--------------------------|--------------------------|
| <u>File K</u> ey Con <u>v</u> ersions <u>H</u> elp | | |
| KeyNo key. | | |
| Generate a public/private key pair | | Generate |
| Load an existing private key file | | Load |
| Save the generated key | Save p <u>u</u> blic key | <u>S</u> ave private key |
| Parameters | | |
| Type of key to generate: O SSH <u>1</u> (RSA) O SSH2 <u>R</u> SA | (ISS | H2 DSA |
| Number of <u>b</u> its 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:

arcutronix

PuTTYgen Generation of SSH-Key

| PuTTY Key Generator | | | | 8 | × |
|---|--|---------------------------------------|------------------------------|--------------|---|
| File Key Conversions | Help | | | | |
| Key | | | | | |
| Public key for pasting in | to OpenSSH authorized | d_keys file: | | | |
| ssh-dss | | | ZUM-04-E | A | |
| rK9t649CDa3infUt+nT | GUTymBRt2X3WY1vZL | ict5vWdLnZ2nqZwnd | ToSQNd6ULD | kzV — | |
| frHvqsn7u2ovQQQ058 AVANvRNHLLfovOvoz | e5Ucjoha6K6f3wRwAz 111R9MBIZavHxAAAAa | 26DE7MCNG6GDChF9 Du196NAcEFHaas/8d | CXAxncEyoc8/ IE70RwR84IKV | AAA Nx1 ▼ | |
| Key fingemrint: | ssh-dss 1023 94·50·77 | '4e:5c f0:41:a5:be:17: | 8a-65-8b-11-22 | .71 | |
| Key assessed | den key 20060207 | .40.00.0.41.00.00.17. | 00.00.00.11.22 | | |
| Key comment: | usa-key-20060307 | | | | |
| Key p <u>a</u> ssphrase: | | | | | |
| Confirm passphrase: | | | | | |
| - Actions | | | | | _ |
| Generate a public/priva | te kev pair | | Generat | e | |
| | | | | | |
| Load an existing private | key file | , | Load | | |
| Save the generated key | / | Save p <u>u</u> blic key | Save private | e key | |
| Parameters | | | | | _ |
| Type of key to generate | e: | | | | |
| O SSH <u>1</u> (RSA) | O SSH2 <u>R</u> SA | SSI | H2 <u>D</u> SA | | |
| Number of <u>b</u> its in a gene | erated key: | | 1024 | | |

| Save private key as | S: | | | | | 8 | ? X |
|---------------------------|-------------------------|--|---|-----|-------|----------------|-------------|
| Speichem in: | C putty | | • | © 🦻 | • 🖭 👏 | | |
| Zuletzt verwendete D | test1.ppk | | | | | | |
| Desktop Eigene Dateien | | | | | | | |
| Arbeitsplatz | | | | | | | |
| Netzwerkumge bung | Dateiname: Dateityp: | private.ppk PuTTY Private Key Files (*.ppk) |) | | • | Speic Abbre | hem chen |

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.

| 🛃 10.0.0.195 - PuTTY | | 1 |
|-----------------------------------|--|---|
| /Login/CoP-FE/Administration/User | Administration/SSH Access/Add SSH Public Key | |
| | | |
| | | |
| | | |
| | | |
| | | |
| Key | jKB+9A3EIeBVJ9L dsa-key-20060307 | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| Exit | | |
| Enter new SSH public key | (a): Alarmiog | 1 |

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 thisd key without a passphrase to protect it?"

6 Configure PuTTY to use SSH

6.1 Session Settings

arcutronix

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.

| 🔀 PuTTY Configuration | n 🗃 🔀 |
|---|--|
| Category: | |
| Session Logging Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation | Basic options for your PuTTY session Specify your connection by host name or IP address "Lost Name (or IP address) Lost Name (or IP address) Protocol. O Baw Leinet Load, save or delete a stored session Saved Sessions |
| Connection Colours Connection Proxy Telnet Rlogin SSH | Default Settings ▲ han02_telnet ▲ sshC0P183 Save sshC0P186 Delete sshC0P195 ▼ |
| Auth Tunnels Bugs | Close <u>w</u> indow on exit: C Always C Never © Only on clean exit |
| About | <u>O</u> pen <u>C</u> ancel |

6.2 Terminal Settings

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

arcutronix

PuTTYgen Generation of SSH-Key

| 🞇 PuTTY Configuration | |
|--|---|
| Putty Configuration Category: Session Logging Comminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours | Options controlling the terminal emulation Set various terminal options ✓ Auto wrap mode initially on DEC Origin Mode initially on Implicit CR in every LF ✓ Use background colour to erase screen Enable blinking text Answerback to ^E: PuTTY |
| Proxy Telnet Riogin | Auto C Force on C Force off Local line editing: Auto C Force on C Force off |
| Auth Tunnels Bugs | Remote-controlled printing Printer to send ANSI printer output to: None (printing disabled) |
| About | Open Cancel |

6.3 Connection Settings

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

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

| 😤 PuTTY Configuration | |
|--|---|
| Category: | |
| Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Connection Proxy Telnet Rlogin SSH Auth Tunnels Bugs | Options controlling the connection Data to send to the server Terminal-type string Auto-login username Cli Sending of null packets to keep session active Seconds between keepalives (0 to turn off) Chevel TCP connection options ✓ Disable Nagle's algorithm (TCP_NODELAY option) |
| About | <u>O</u> pen <u>C</u> ancel |

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:

arcutronix

arcutronix

PuTTYgen Generation of SSH-Key

| 🞇 PuTTY Configuratio | n 😑 🔀 |
|---|---|
| Category: | |
| Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Proxy Telnet Rlogin SSH Auth Tunnels Bugs | Options controlling SSH authentication Authentication methods Attempt TIS or CryptoCard authentication (SSH1) ✓ Attempt "keyboard-interactive" authentication (SSH2 Authentication parameters Allow agent forwarding Allow attempted changes of username in SSH2 P:: are Key file for authentication: C:\temp\putty\private.ppk |
| About | Open Cancel |

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

| 😤 PuTTY Configuration | n 🔤 🗙 |
|---|--|
| Category: | |
| Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Proxy Telnet Rlogin SSH Auth Tunnels Bugs | Options controlling SSH authentication Authentication methods Attempt TIS or CryptoCard authentication (SSH1) ✓ Attempt "keyboard-interactive" authentication (SSH2 Authentication parameters Allow agent forwarding Allow attempted changes of username in SSH2 Private key file for authentication: C:\temp\putty\private.ppk Browse |
| About | Open Cancel |

7 Further help

For further help, please contact arcutronix GmbH at

service@arcutronix.com or meet us at the Internet

www.arcutronix.com

arcutronix GmbH
Garbsener Landstr. 10
D-30419 Hannover
Germany +49 511 277 2700
sales@arcutronix.com
www.arcutronix.com