

SSH Key Generation (PuTTY version)

Last update: May 24, 2021 (verified with PuTTY 0.75)

Introduction

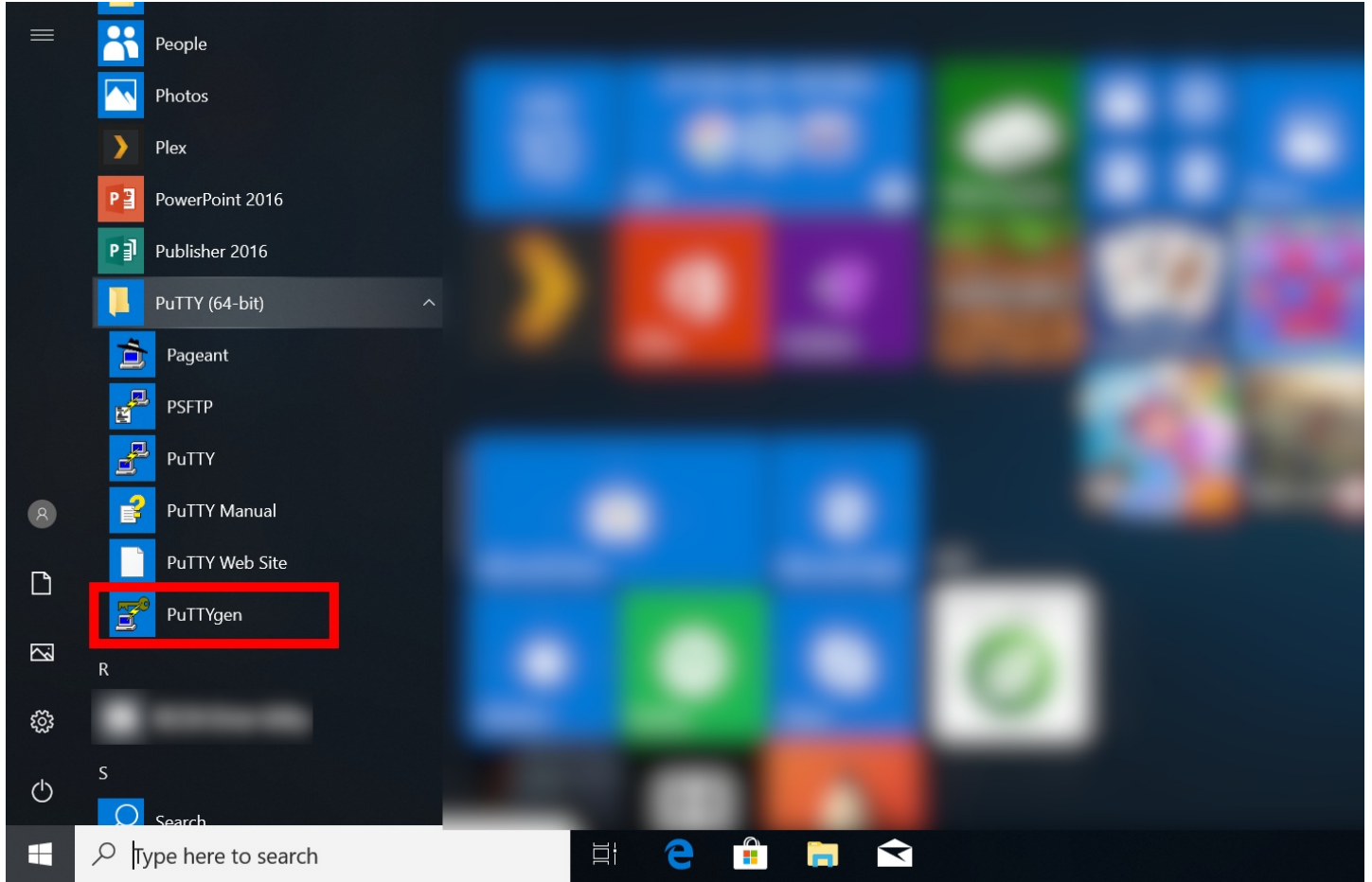
The aim of this page is to explain how to login to RCCS supercomputer using PuTTY and PuTTYgen.

Install PuTTY

You can download PuTTY at its official site (<https://www.putty.org>). MSI installer version of the latest stable release available in [this page](#) maybe the most standard way to install PuTTY. If you already have PuTTY but not PuTTYgen, you can install PuTTYgen (puttygen.exe) from the "Alternative binary files" section of the download page.

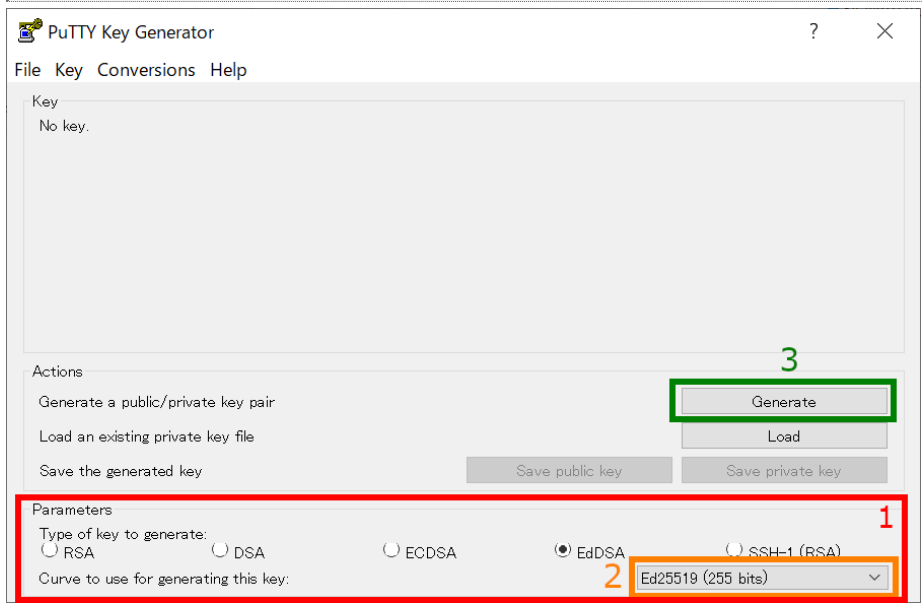
SSH key generation (PuTTYgen)

Launch PuTTYgen



PuTTYgen can be launched from Windows start menu.

Key generation (1) - Key type



You may see PuTTYgen window like above.

1. Choose Key Type

Ed25519, ECDSA (256, 384, 521 bits), and RSA 4096 bits * of keys are recommended in RCCS. Please choose Ed25519 if you have no preference. **NOTE: Ed448 is not yet available at RCCS frontend nodes. Please don't choose Ed448!**
*PuTTY 0.74 or before does not support SHA2 algorithms of RSA (rsa-sha2-256/512). Therefore, if SHA1 algorithm (ssh-rsa) is disabled in the near future, it may cause an RSA authentication problem. (Note: the RSA key format itself is not related with those SHA1 and SHA2 algorithms; you may not need to generate new key if you already have enough-long RSA key.)

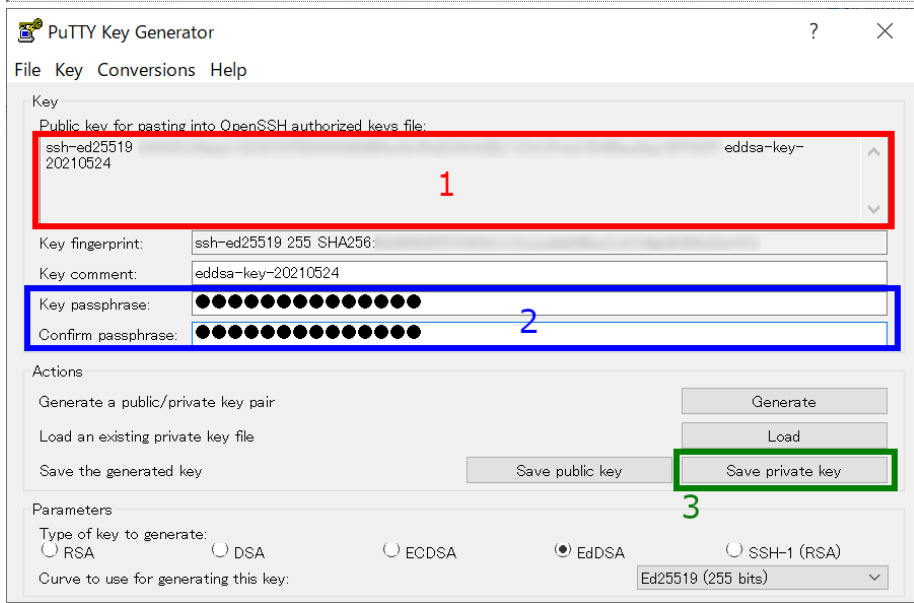
2. Choose Key Length (ECDSA or RSA case)

In case of ECDSA or RSA type, you may find optional item at the position specified by "2". Please choose/input value there.

3. Start Generation of Key

Once you click the "Generate" button, the key generation will begin. You need to move mouse cursor around to proceed the key generation after clicking the button.

Key generation(2) - Set passphrase, then save the keys



PuTTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized keys file:

```
ssh-ed25519  
20210524
```

Key fingerprint: ssh-ed25519 255 SHA256:

Key comment: eddsa-key-20210524

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)

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

Once the key generation completed, the appearance of the window will change like above.

1. OpenSSH type public key

The public key shown as a string in this field is what we need. Extract all the contents in this field into notepad or others, and then save it! (Do not miss ssh/ecdsa- part in the beginning!) Note: you don't need public key from "Save public key" button; we need only OpenSSH format one.

You can rebuild public keys via "Load" button or "Conversion" menu if you still have private key. (If you lost the private key, you need to generate a new key.)

2. Set passphrase for private key

You can set passphrase for private key here. We, RCCS, recommend passphrase of 10 or more characters containing 4 types of characters - "lower-case", "upper-case", "number", and "symbol".

3. Save the private key

After setting passphrase, click "Save private key" button to save the key. Easy-to-understand name such as "rccs.ppk" or "ccfep.ppk" may be a good choice. (NOTE: THE PRIVATE KEY FILE MUST BE KEPT SECRET!)

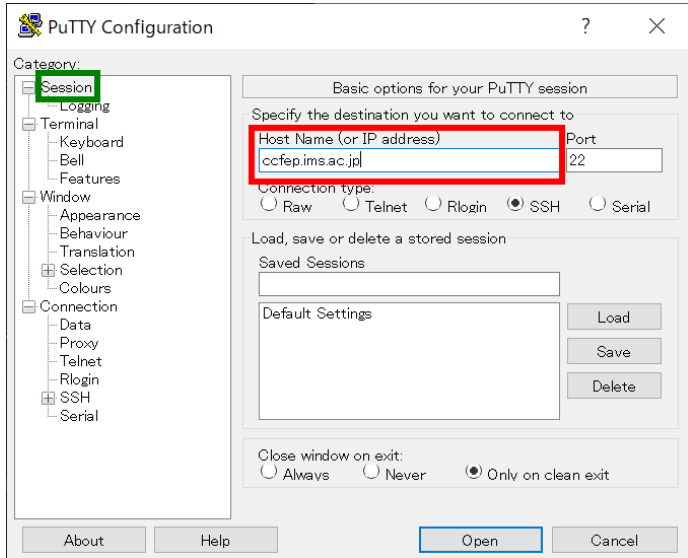
Register Public Key (Common)

You need to register the public key before login. Please register your public key according to the instructions in <https://ccportal.ims.ac.jp/en/account>.

Please note that the public key here is an OpenSSH type one, not the one from "Save public key" button.

Login (PuTTY)

Launch PuTTY and set destination



PuTTY Configuration

Category:

- Session
- Logging
- Terminal
- Keyboard
- Bell
- Features
- Window
- Appearance
- Behaviour
- Translation
- Selection
- Colours
- Connection
- Data
- Proxy
- Telnet
- Rlogin
- SSH
- Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port

Connection type:

Raw Telnet Rlogin SSH Serial

Load, save or delete a stored session

Saved Sessions

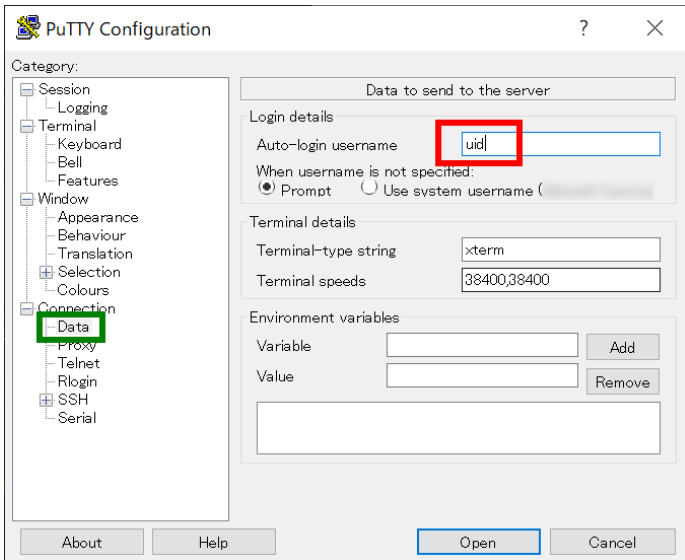
Default Settings

Close window on exit:

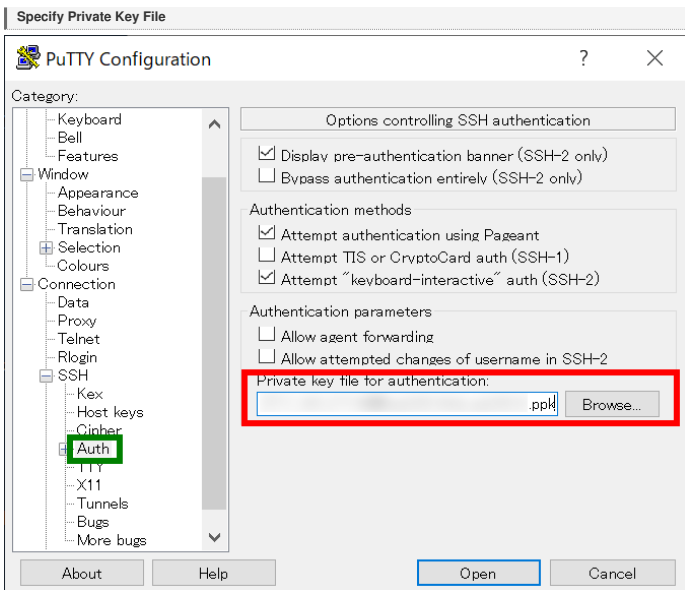
Always Never Only on clean exit

Launch PuTTY, input `ccfep.ims.ac.jp` in "Host Name (or IP address)" text box. (Do not push "Open" now!)

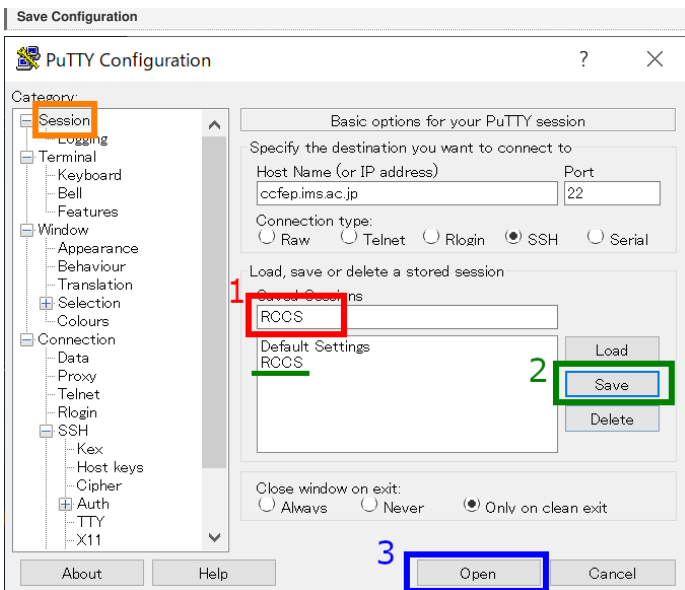
Specify user name



Move to "Data" in "Connection" item. You can set username in "Auto-login username" textbox. Please input **RCCS user id (three-letter ID given by RCCS)**. You can skip this step. You need to input username upon authentication in this case.

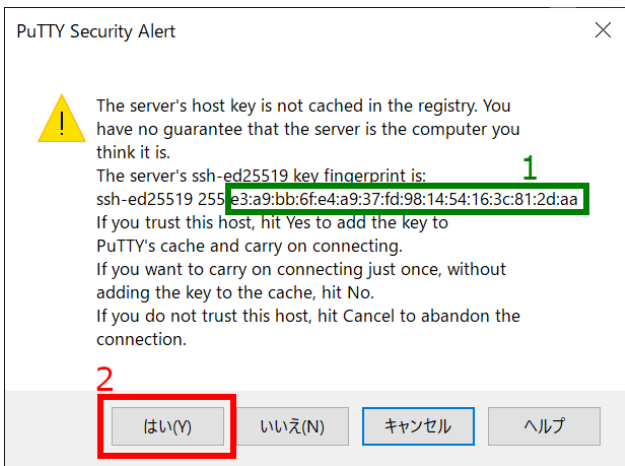


Move to "Auth" menu in "SSH" menu under "Connection". The generated private key file (.ppk) should be specified in this menu.



Although you can connect to RCCS servers by clicking "Open" button, you should save the configuration before trying to connect. Move back to "Session", and **give a name to this connection in textbox ("1")**, then **click "Save" button to save it ("2")**. The saved connection name would appear in the list. **Finally, click "Open" to begin connection.**

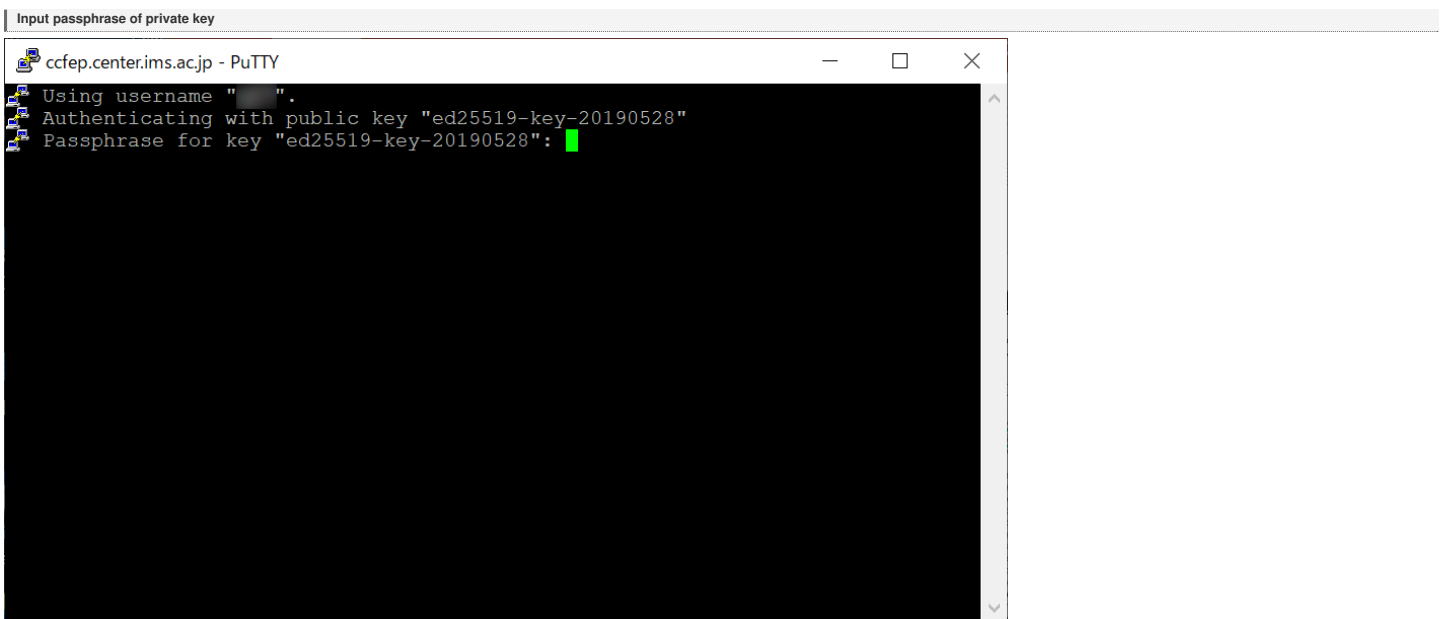
Alert message upon first connection



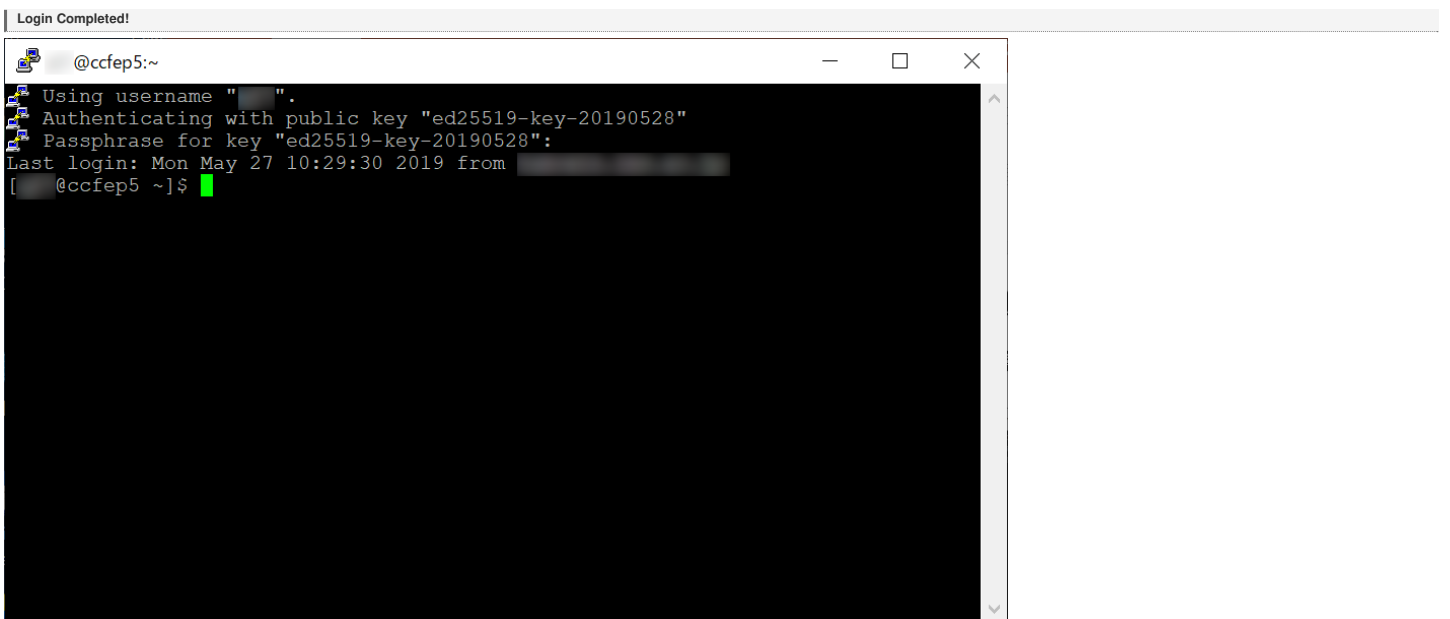
Dialog like above would be shown upon first connection. Please check the fingerprint (1); this must match with either of the fingerprint listed below.

- ▶ ad:de:79:30:81:b0:b1:6a:17:f5:6f:ea:44:b4:3b:de (MD5)
- ▶ e3:a9:bb:6f:e4:a9:37:fd:98:14:54:16:3c:81:2d:aa (MD5)
- ▶ 07:7e:df:7b:16:47:a8:f5:7c:48:b0:a3:d3:86:71:6a (MD5)
- ▶ wnEM30z4AxyDJ9XIUdGr2PINeivFRR8v5krXHEmdU (SHA256)
- ▶ 0KL38Yn/kBee1pAuxyKwenEwXjIPxr9ZElolVqXvbl (SHA256)
- ▶ Nhg+9Lgj3XeuW//A/j7jggUJllxWehryCtStip1Dir (SHA256)

Click Ok button if the fingerprint is a valid one.



Window like above would be shown if connection to server is succeeded. You then need to input passphrase to use your private key. (Note: if you register the key to Pageant beforehand, you are able to skip this step.)



If your key settings are OK, you can login to our frontend server like above.