SSH key creation and login (PuTTY version)

National Institutes of Natural Sciences

Okazaki Research Facilities

Research Center for Computational Science (RCCS)

(Verified with PuTTY 0.80)

Changelog

- Jul 10, 2019 First version
- Feb 2, 2021 Update (recommended key types etc.)
- May 24, 2021 Update for PuTTY 0.75
- Jan 5, 2022 Verified with PuTTY 0.76
- Dec 20, 2022 Update for PuTTY 0.78 and our new system
- Jun 2, 2023 Minor fix of wording
- Jan 18, 2024 Verified with PuTTY 0.80

Introduction

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

Table of Contents

- Install PuTTY
- SSH key creation
- Register public key
- Login

Install PuTTY

PuTTY can be downloaded from the following site:

https://www.chiark.greenend.org.uk/~sgtatham/putty/

The latest version of PuTTY can be downloaded at:

https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

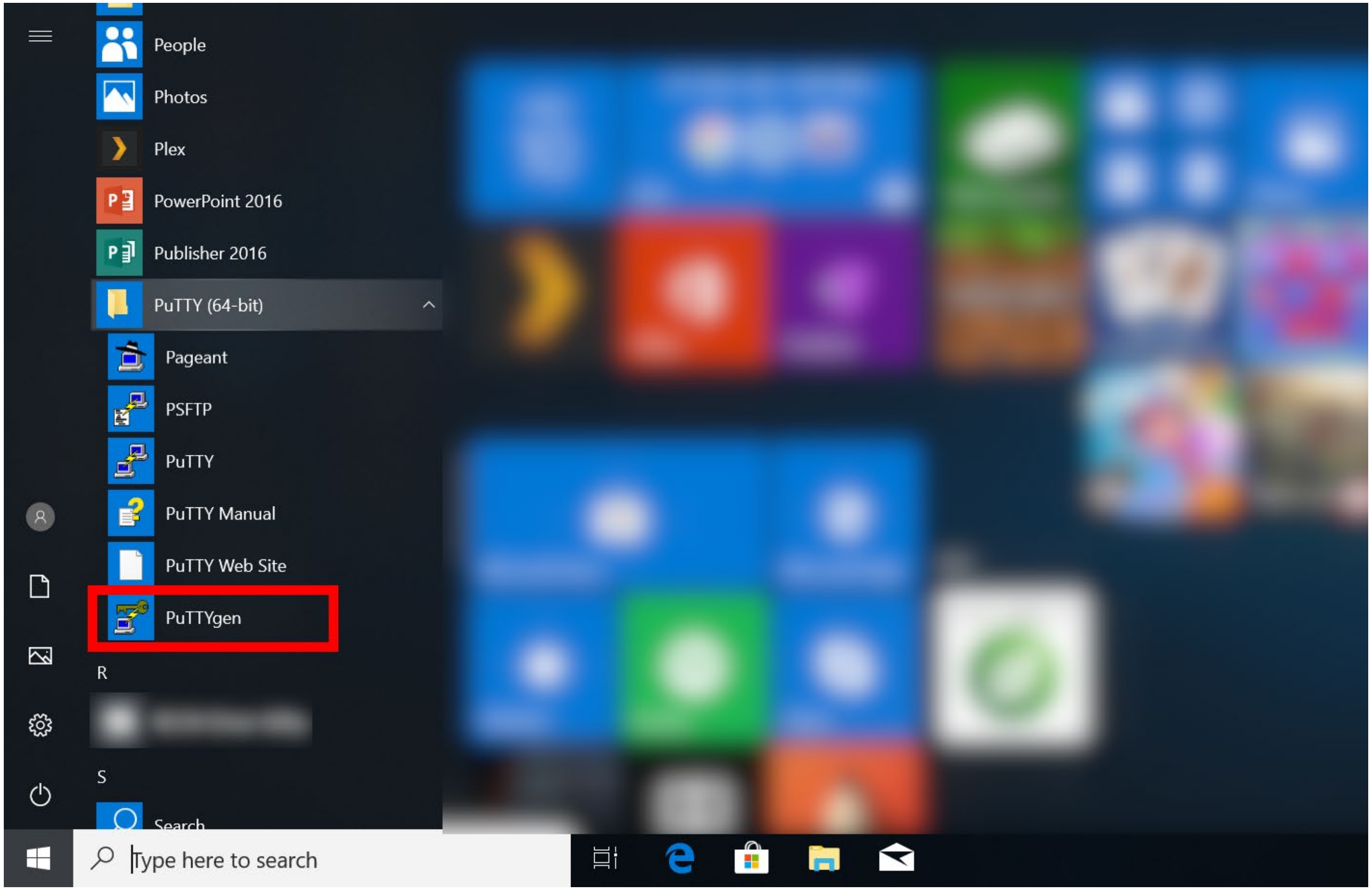
MSI (Windows Installer) version is recommended.

We will use PuTTY and PuTTYgen.

If you already have PuTTY but not PuTTYgen, please install standalone version of PuTTYgen (puttygen.exe) from the link in “Alternative binary files” section of the download site.

SSH key creation (1)

Launch PuTTYgen. If you installed MSI installer version, PuTTYgen can be found in Start Menu.



SSH key creation (2)

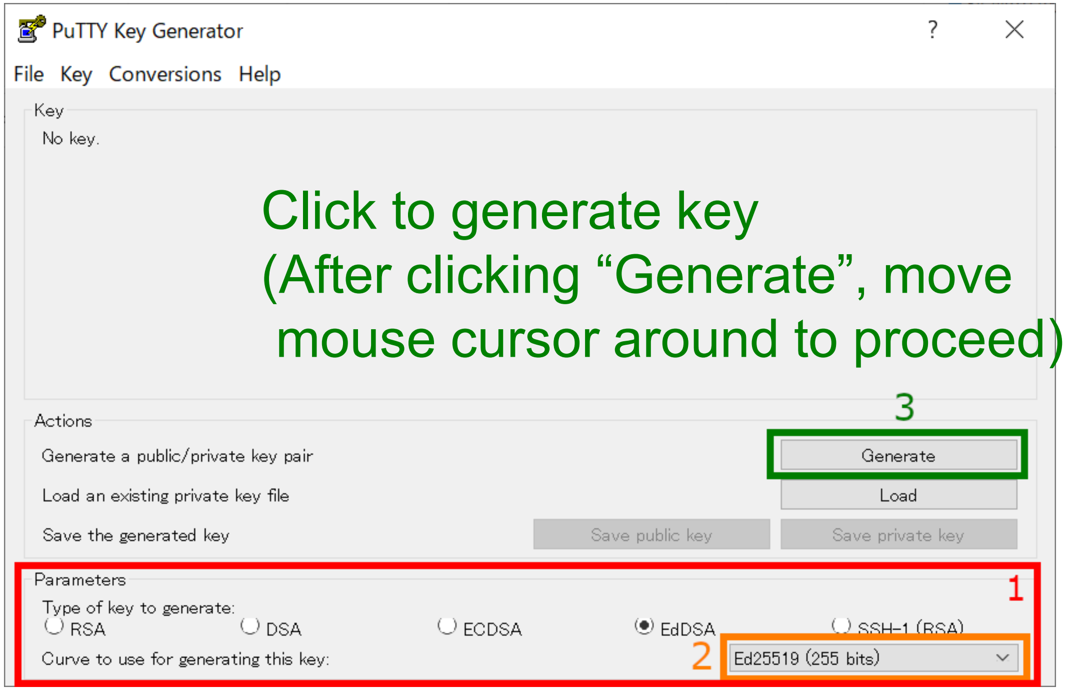
RCCS recommends following types of keys.

- Ed25519 (select EdDSA of 255 bits)
- ECDSA (256, 384, or 521 bits)
- RSA 4096 bits (select RSA & modify number at lower right to 4096)

Don’t choose Ed448!
Login servers don’t support that!

Choose Ed25519 if you have no preference.

You need PuTTY 0.75 or later
to use RSA key!



No key.

Generate a public/private key pair

Load an existing private key file

Save the generated key

Type of key to generate:
○ RSA ○ DSA ○ ECDSA ● EdDSA ○ SSH-1 (RSA)

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

Click to generate key
(After clicking “Generate”, move
mouse cursor around to proceed)

Select key type

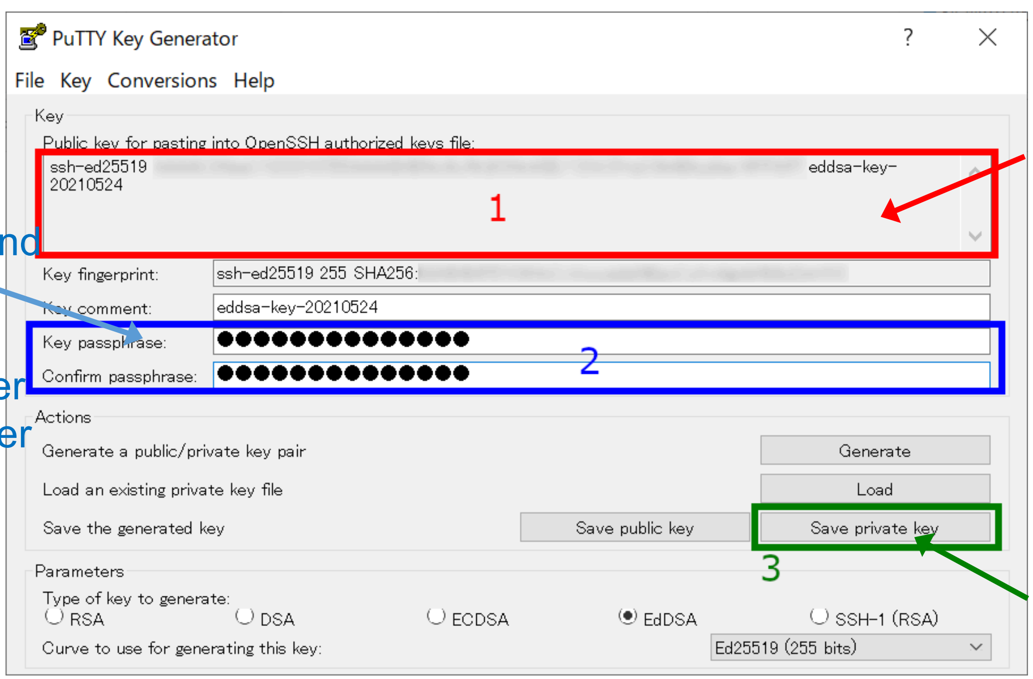
Choose key length (RSA, ECDSA, EdDSA)

SSH key creation (3)

Once key generation finished, new items will be shown in the window.

RCCS recommends passphrase of 10 or more characters and containing all the following 4 types.

- lower-case character
- upper-case character
- number
- symbol



Key

Public key for pasting into OpenSSH authorized keys file:

```
ssh-ed25519 [redacted] eddsa-key-
20210524
```

Key fingerprint: ssh-ed25519 255 SHA256:[redacted]

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)

This is the public key we need. You should save this key in a file. **(Please copy whole the key. This window is often too small for some types of keys.)**

Click to save the private key.
You might want to choose easy-to-understand filename such as rccs.ppk or ccfep.ppk.

- Generated private key file must be kept secret.
- OpenSSH type private key can be obtained from “Conversions” menu (if needed).
- Public key can be restored from the private key; try “Load” button.
- If you lost the private key, you need to generate new one...

Register Public Key

Before login, you need to register the public key.

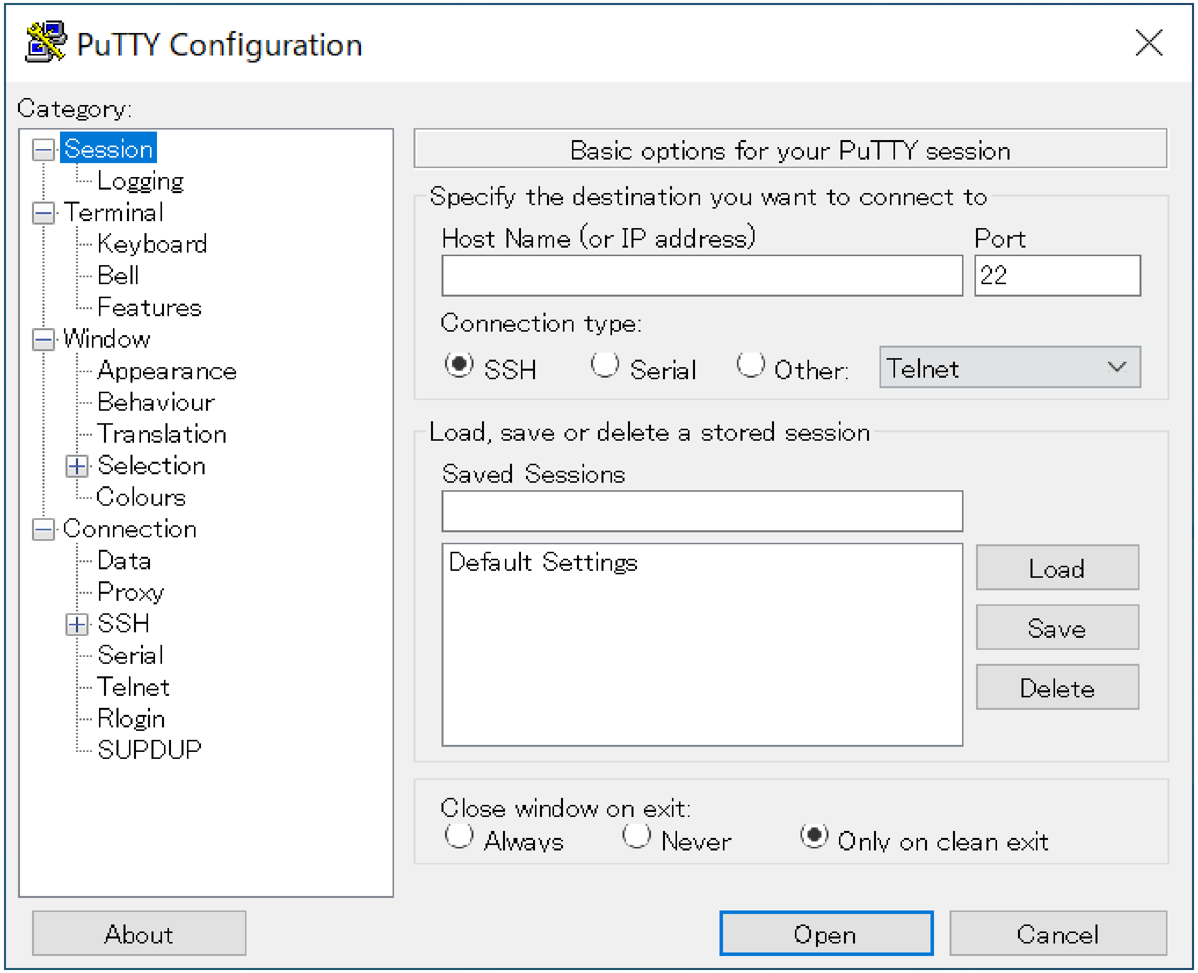
The procedure of the public key registration is available from the following link.
https://ccportal.ims.ac.jp/en/account/

Don’t use the key from “Save public key” button of PuTTYgen.
Key displayed at “Public key for pasting into OpenSSH...” part of PuTTYgen window is the one what we expect.

The private key file must be kept secret.

Login (1)

Did you register public key? OK, let’s launch PuTTY.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address)

Port: 22

Connection type:

● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions

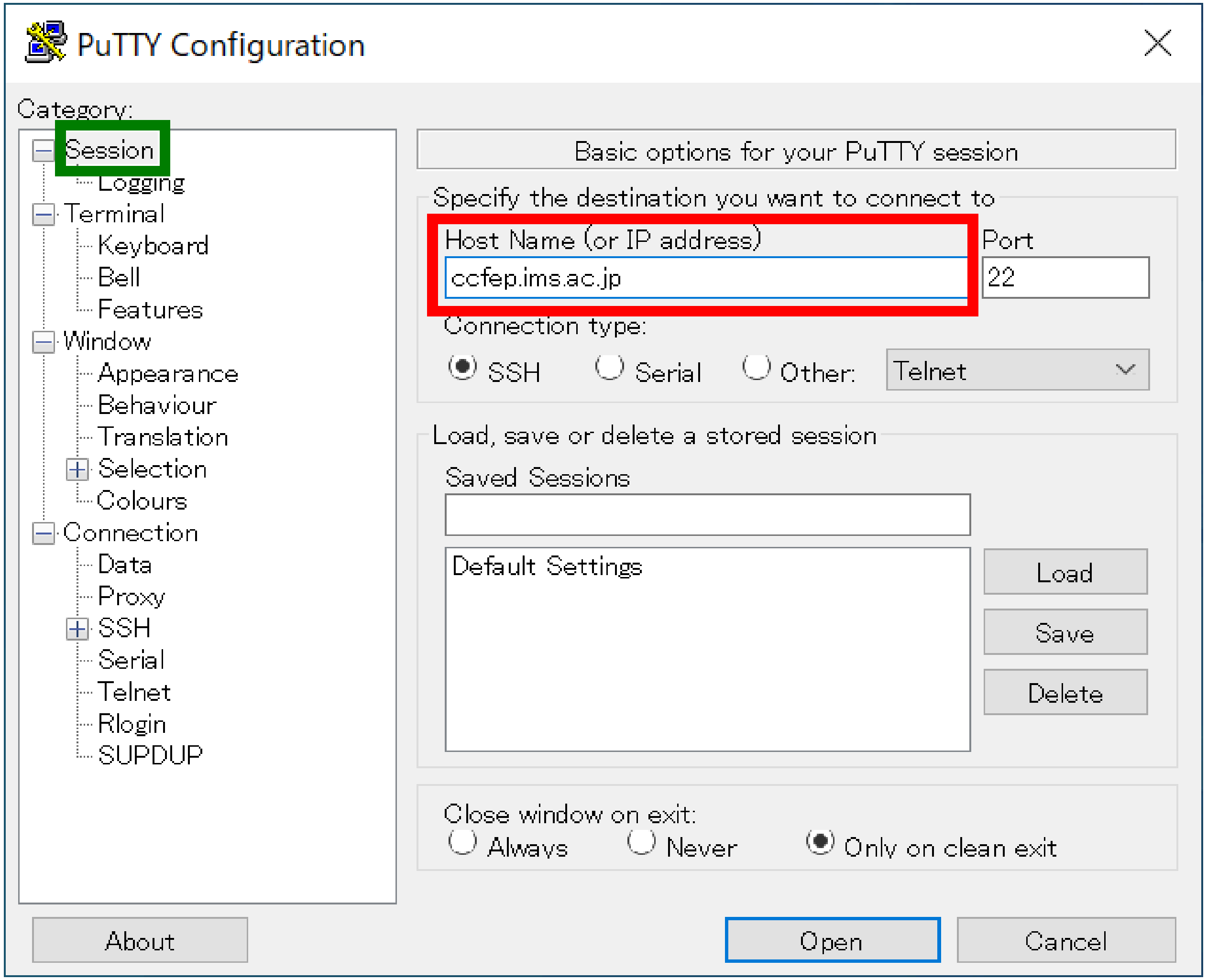
Default Settings

Close window on exit:

○ Always ○ Never ● Only on clean exit

Login (2)

In [Session], type “ccfep.ims.ac.jp” in the Host Name box.



PuTTY Configuration

Category:

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

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): ccfep.ims.ac.jp

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

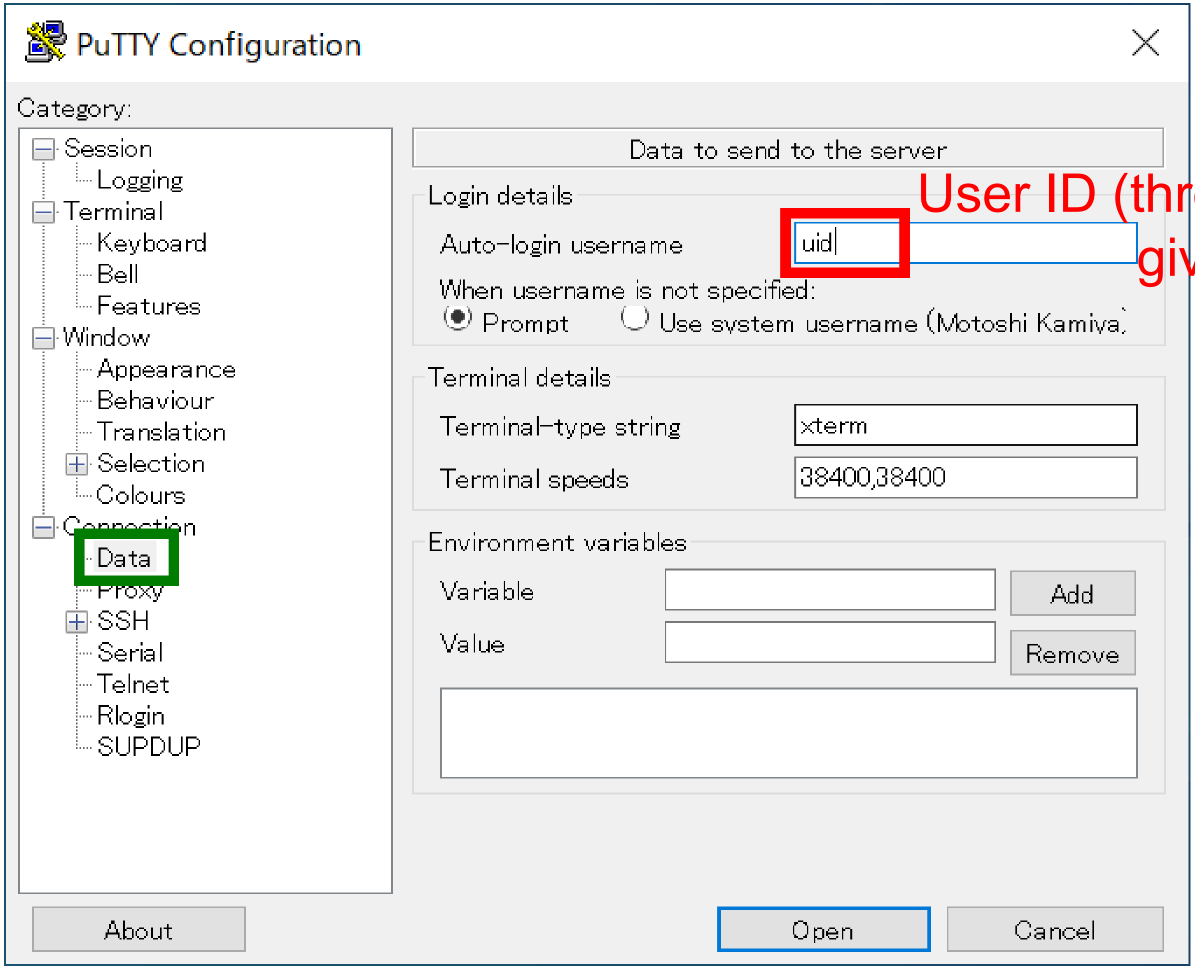
Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Login (3)

Move to [Connection] -> [Data] and fill your ID in the username box.



PuTTY Configuration

Category:

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

Data to send to the server

Login details

Auto-login username: uid

When username is not specified:

● Prompt ○ Use system username (Motoshi Kamiya)

Terminal details

Terminal-type string: xterm

Terminal speeds: 38400,38400

Environment variables

Variable:

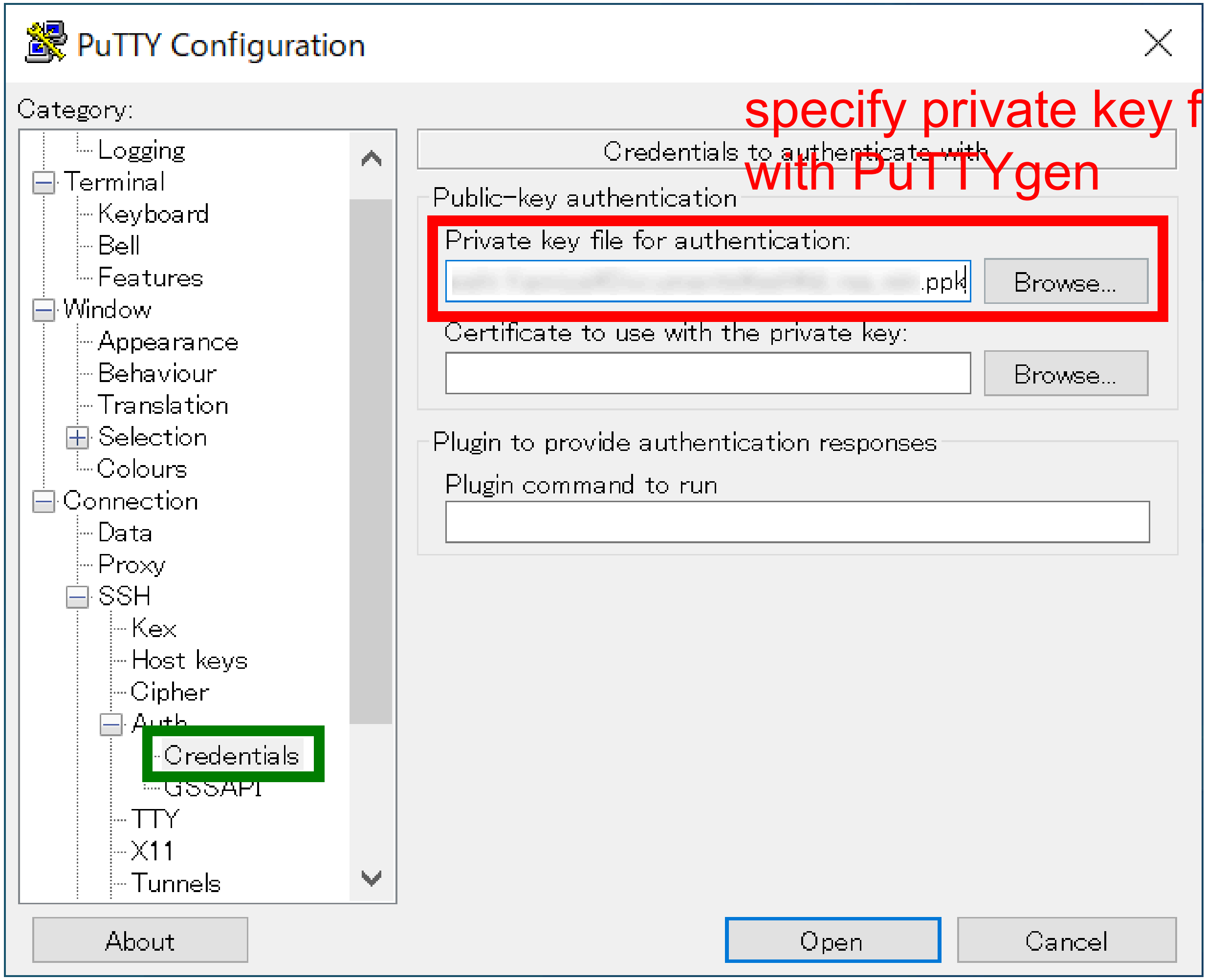
Value:

User ID (three letter ID given by RCCS)

(This step can be skipped. In that case, you will be asked upon connection.)

Login (4)

Move to [Connection] -> [Data] -> [SSH] -> [Auth] -> [Credentials] and specify private key (.ppk file)



PuTTY Configuration

Category:

Credentials to authenticate with

Public-key authentication

Private key file for authentication: [redacted].ppk [Browse...]

Certificate to use with the private key: [Browse...]

Plugin to provide authentication responses

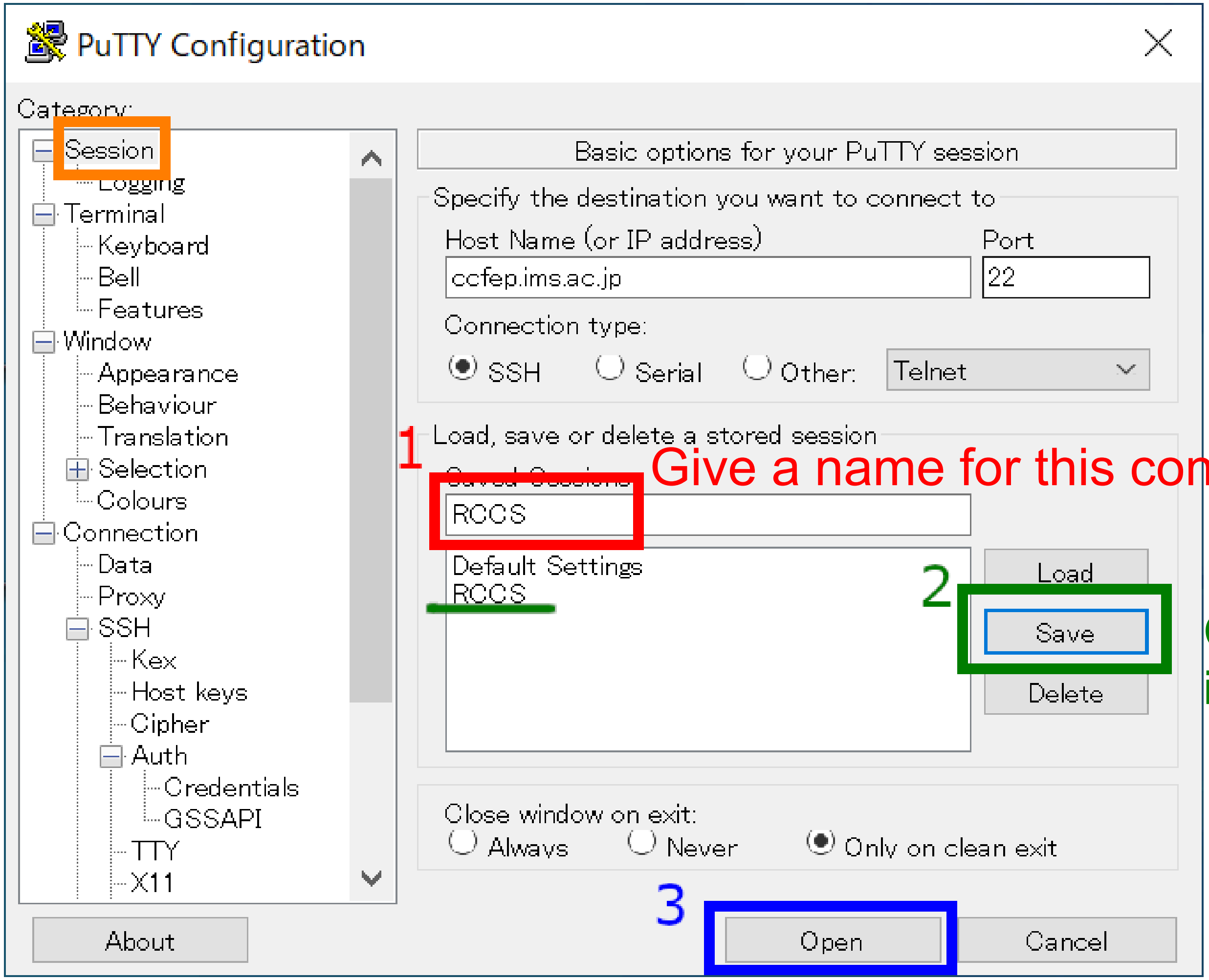
Plugin command to run

specify private key file generated with PuTTYgen

If [Credentials] menu item does not exist, the private key file field can be found in [Connection] -> [Data] -> [SSH] -> [Auth] menu item.

Login (5)

Move to [Session], save settings, and then login.



PuTTY Configuration

Category:

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): ccfep.ims.ac.jp

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions: RCCS

Default Settings
RCCS

Close window on exit: ○ Always ○ Never ● Only on clean exit

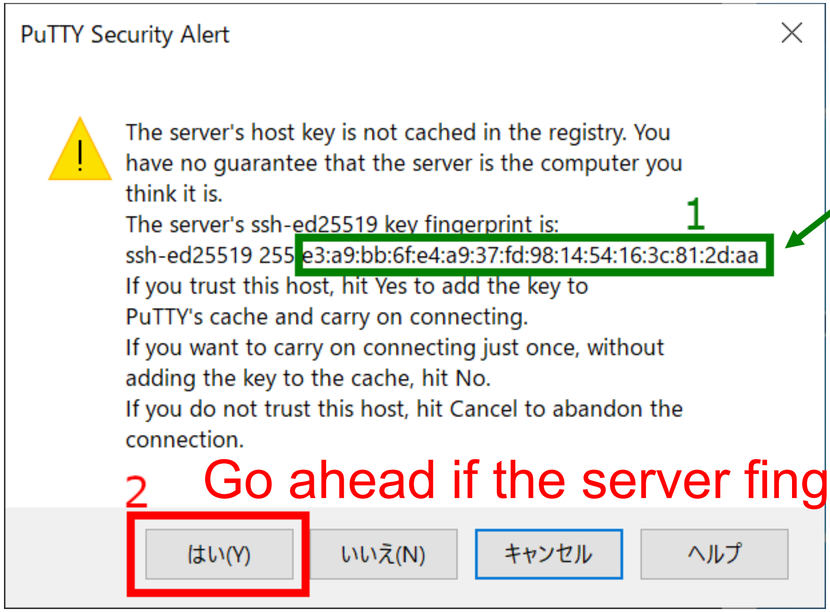
1 Give a name for this connection

2 Click to save into the list

3 Let’s login!

Login (6)

Upon first connection, alert message will be shown.



PuTTY Security Alert

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255 e3:a9:bb:6f:e4:a9:37:fd:98:14:54:16:3c:81:2d:aa
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

Check the fingerprint; this must match with either of the fingerprint in the list below.

Go ahead if the server fingerprint is valid.

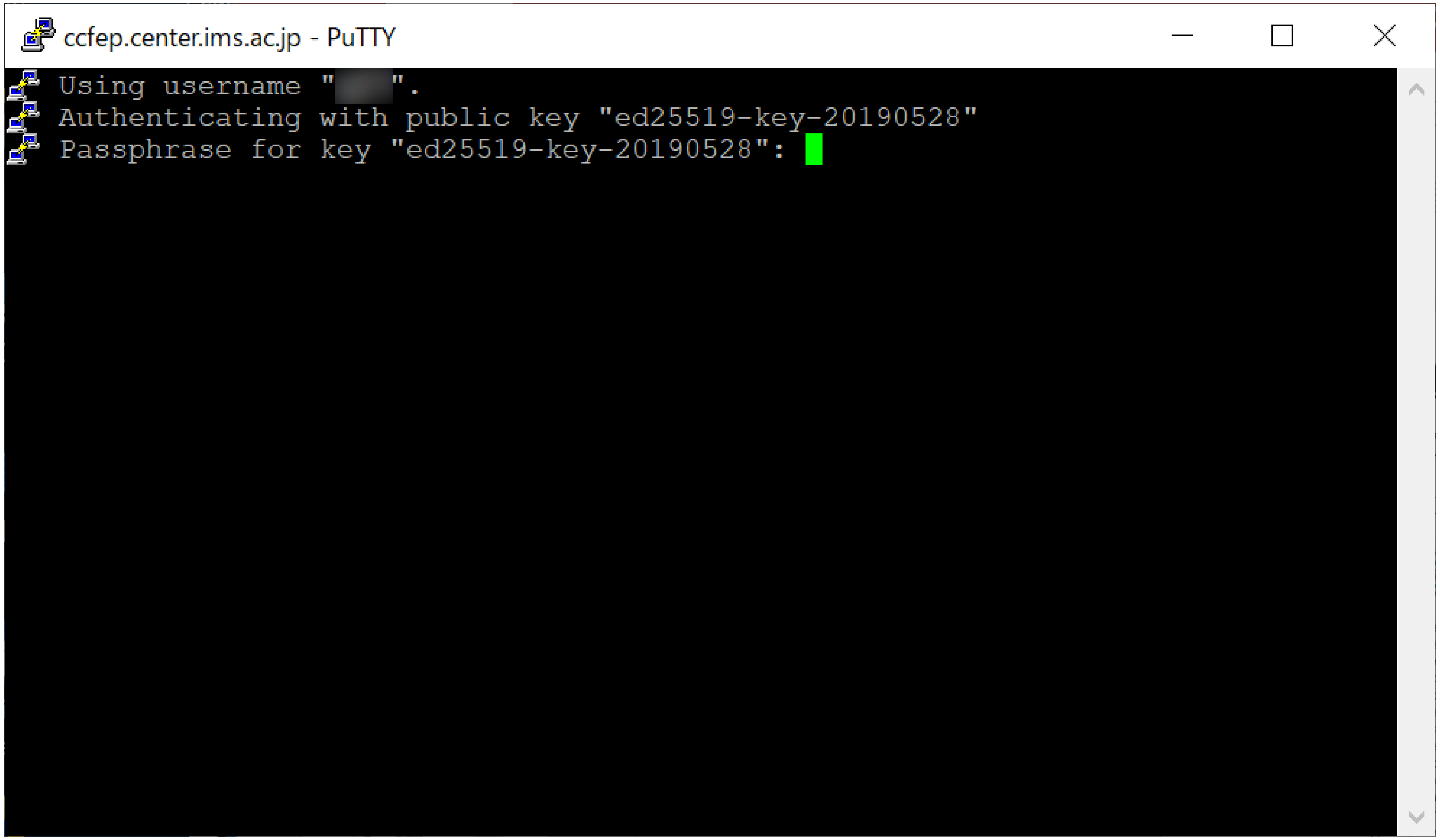
Fingerprints of valid server keys

- ad:de:79:30:81:b0:b1:6a:17:f5:6f:ea:f4: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)

- wnEM30z4AxyDJ9XI/DdGr2PINeoivFRR8v5krXHEmdU (SHA256)
- 0KL38Yn/kBee1pAuxyKwenEwXjtPxr9ZEIoIfVqXvbI (SHA256)
- Nhg+9Lgj3XeuW//A/j7jqgUJlIxWehryCtStIp1Dirs (SHA256)

Login (7)

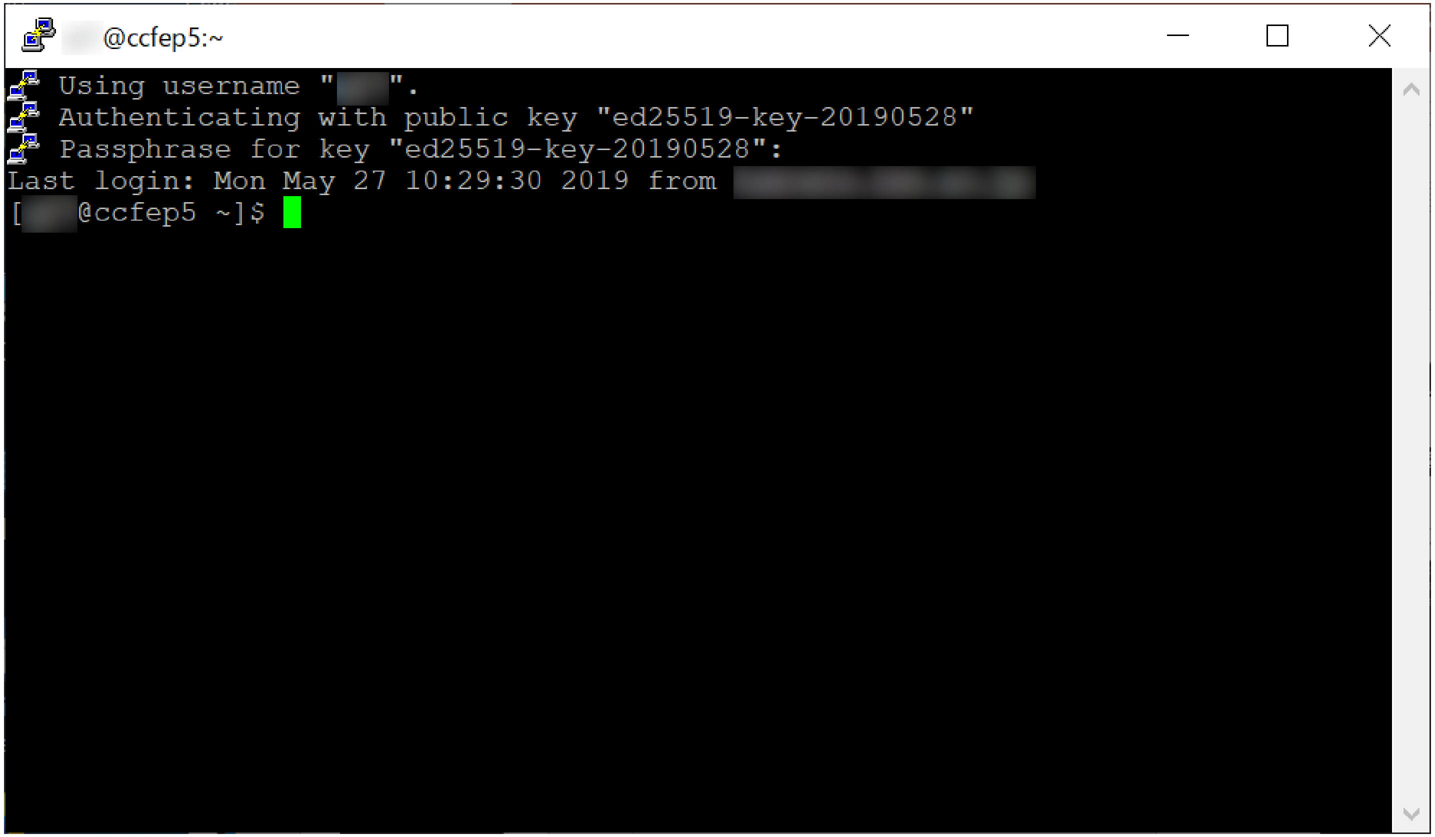
You will be asked passphrase of private key. Type it.



```
Using username "[redacted]".
Authenticating with public key "ed25519-key-20190528"
Passphrase for key "ed25519-key-20190528":
```

Login (8)

Once you typed correct passphrase, login to RCCS login server will be granted.



```
Using username "[redacted]".
Authenticating with public key "ed25519-key-20190528"
Passphrase for key "ed25519-key-20190528":
Last login: Mon May 27 10:29:30 2019 from [redacted]
[[redacted]@ccfep5 ~]$
```

Note: if you launch Pageant and your key is registered, passphrase won’t be asked upon connection. (You need to type passphrase upon registration to Pageant.)