SSH key creation and login (PuTTY version)

National Institutes of Natural Sciences

Okazaki Research Facilities

Research Center for Computational Science (RCCS)

(Confirmed with PuTTY 0.71)

Changelog

- Jul 10, 2019   First version

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.putty.org/

(Follow the link in the "Download PuTTY" section.)

MSI (Windows Installer) version is recommended.

We will also 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.
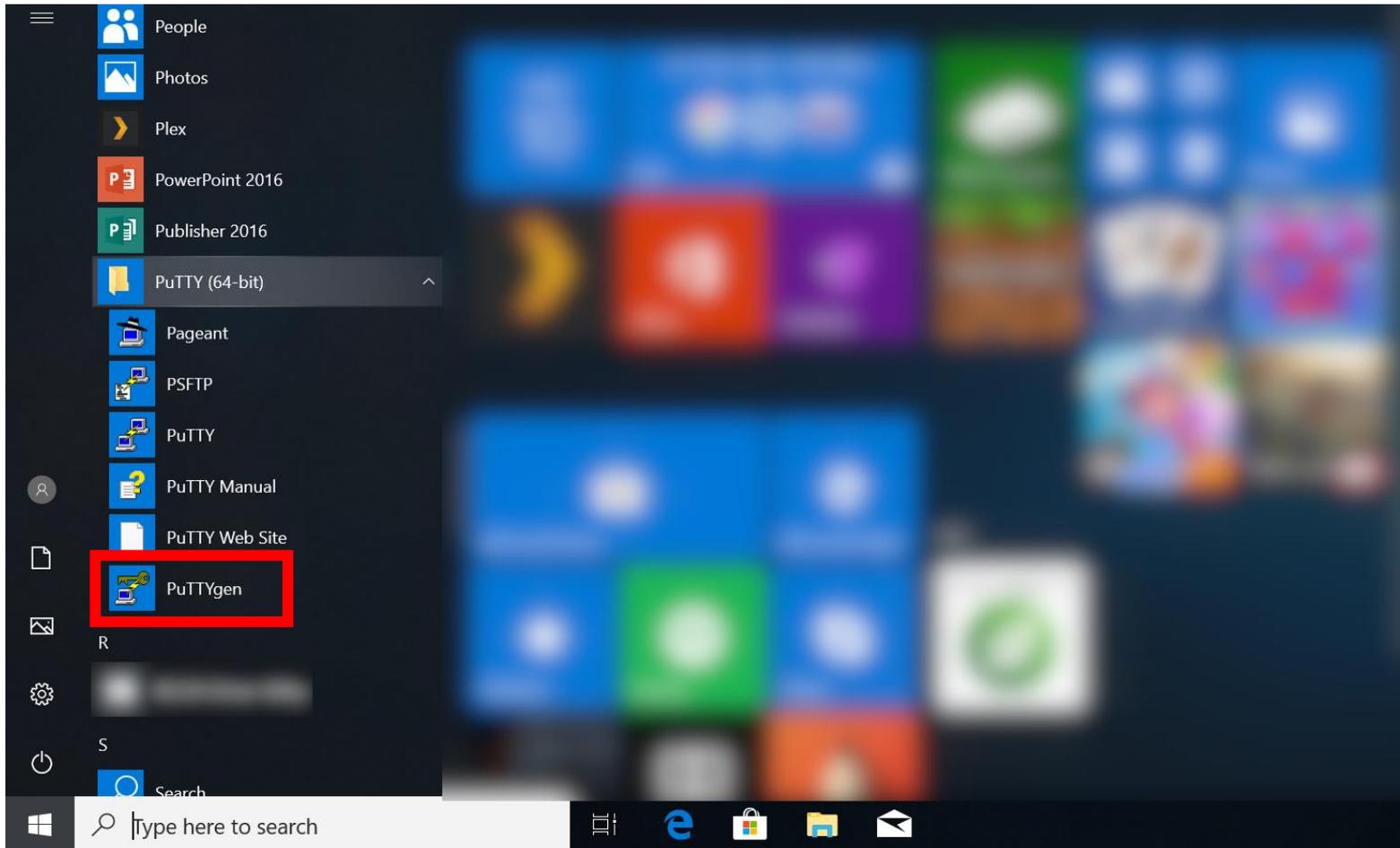
SSH key creation (2)

RCCS recommends following types of keys.

- RSA 4096 bits (select RSA & modify number at lower right to 4096)
- ECDSA (256, 384, or 521 bits)
- ED25519

Use RSA 4096 if you have no preference.
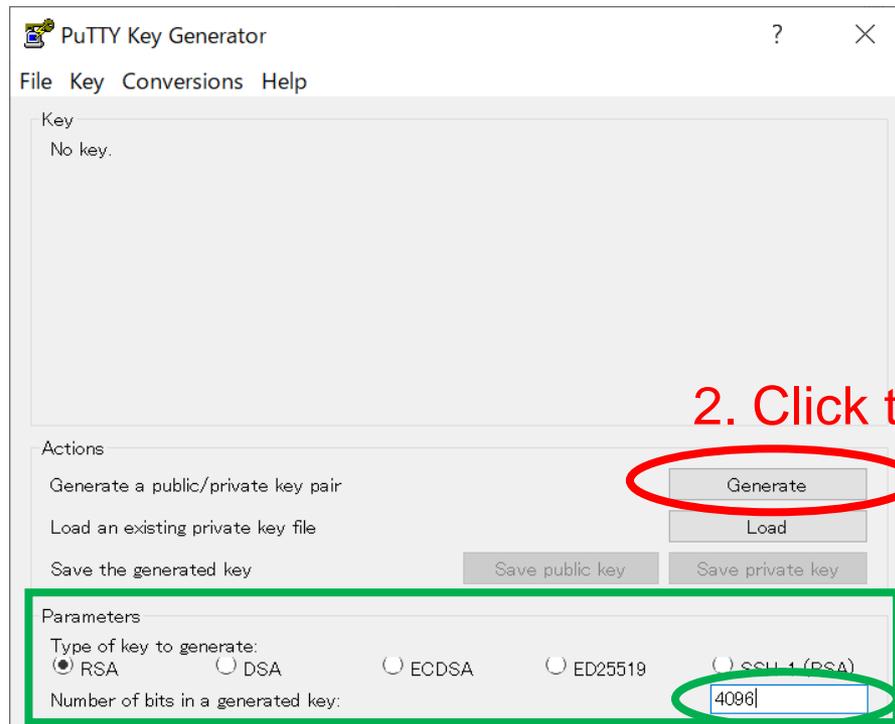
2. Click to generate key

1. Select key type

鍵の長さ指定

(3. After clicking "Generate", move mouse cursor around.)

SSH key creation (3)

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

2. RCCS recommends passphrase of 10 or more characters and containing all the following 4 types of characters.
- lower-case character
- upper-case character
- number
- symbol
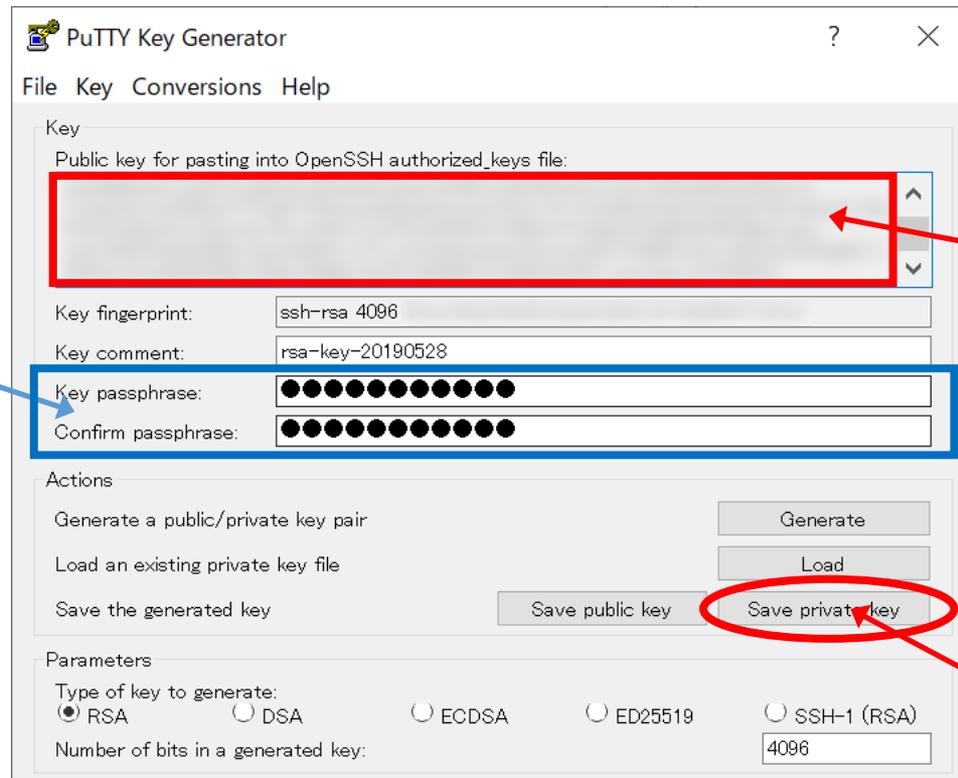
1. This is the public key we need. You should save this key in a file. **(Please copy whole the key. This window is often too small for some types of keys.)**

3. 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.

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.
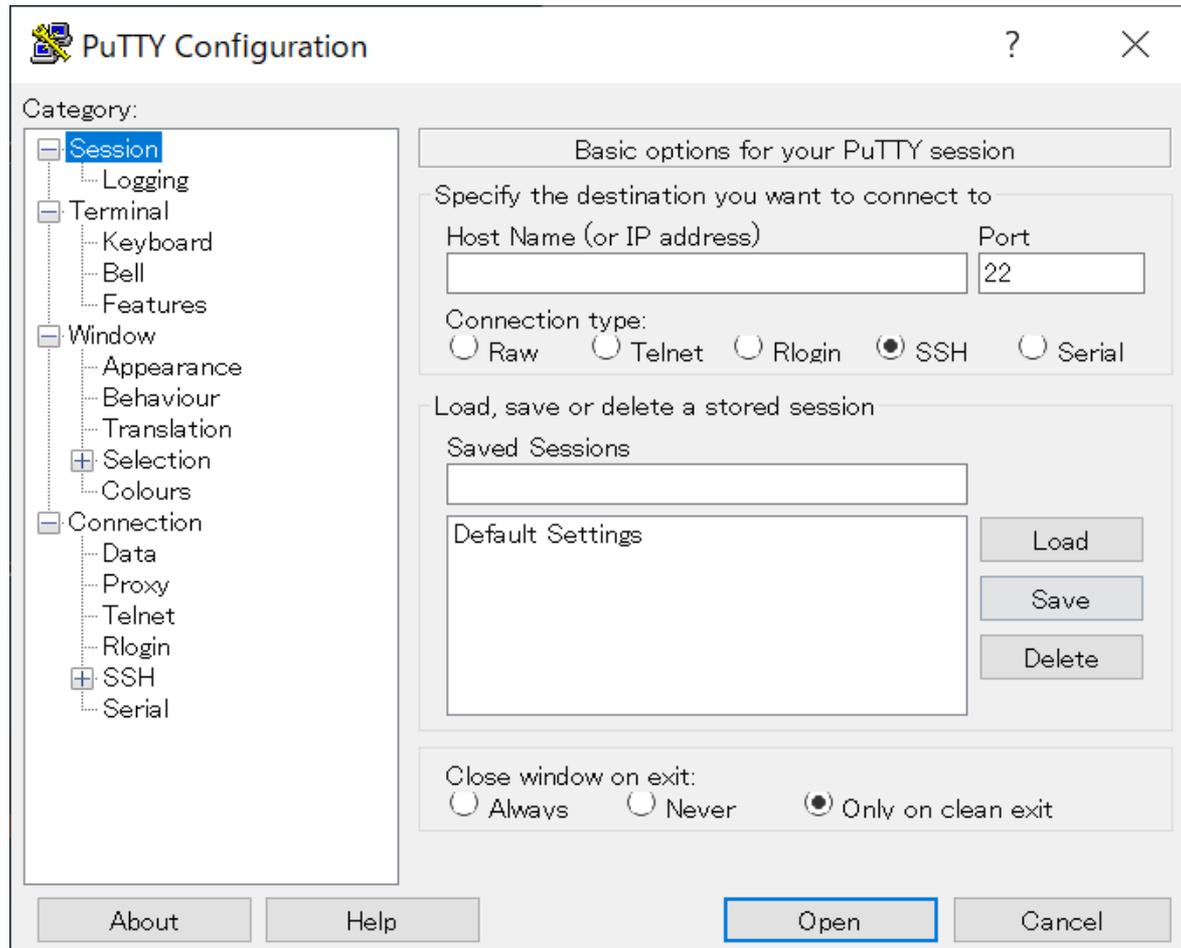
Login (2)

In [Session], type "ccfep.ims.ac.jp" in the Host Name box.
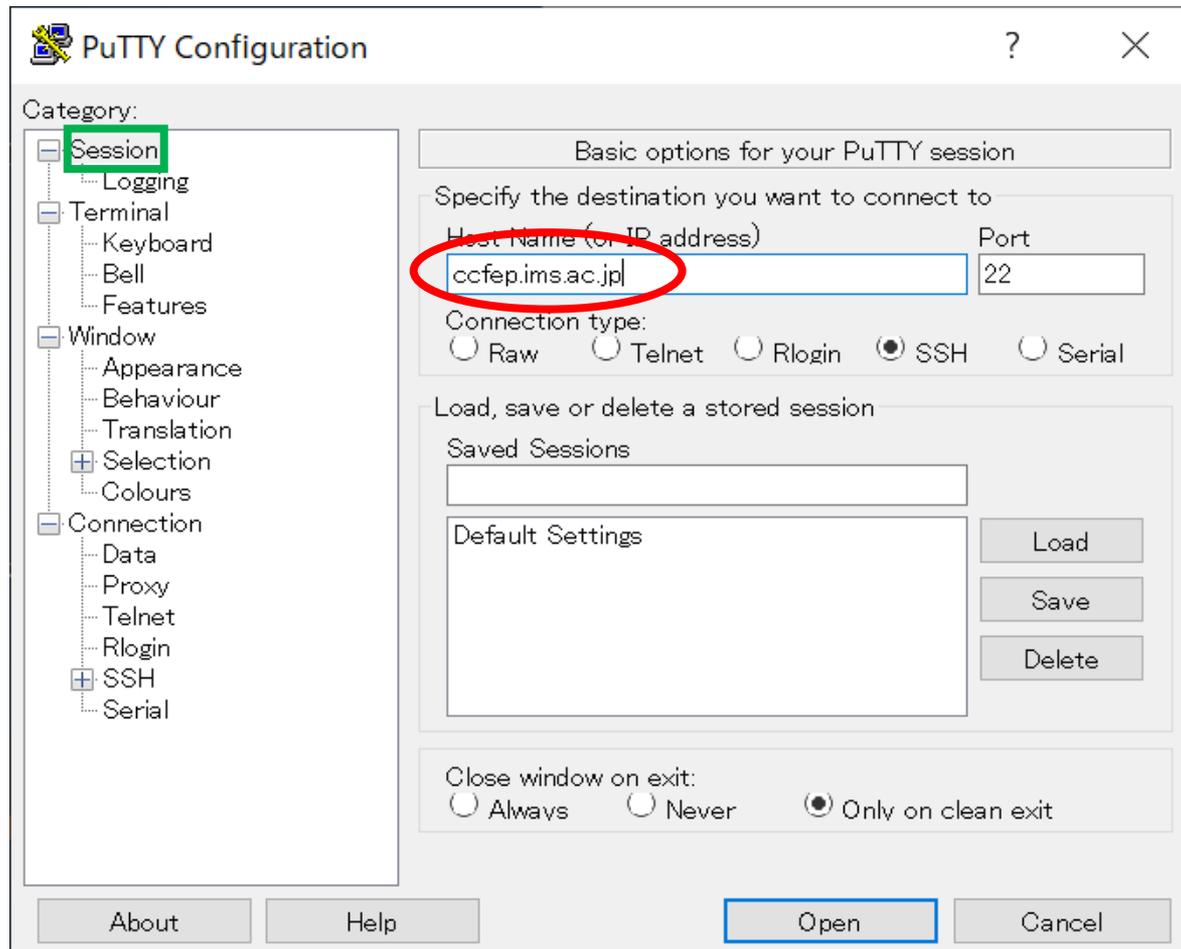
Login (3)

Move to [Connection] -> [Data] and fill your ID in the username box.
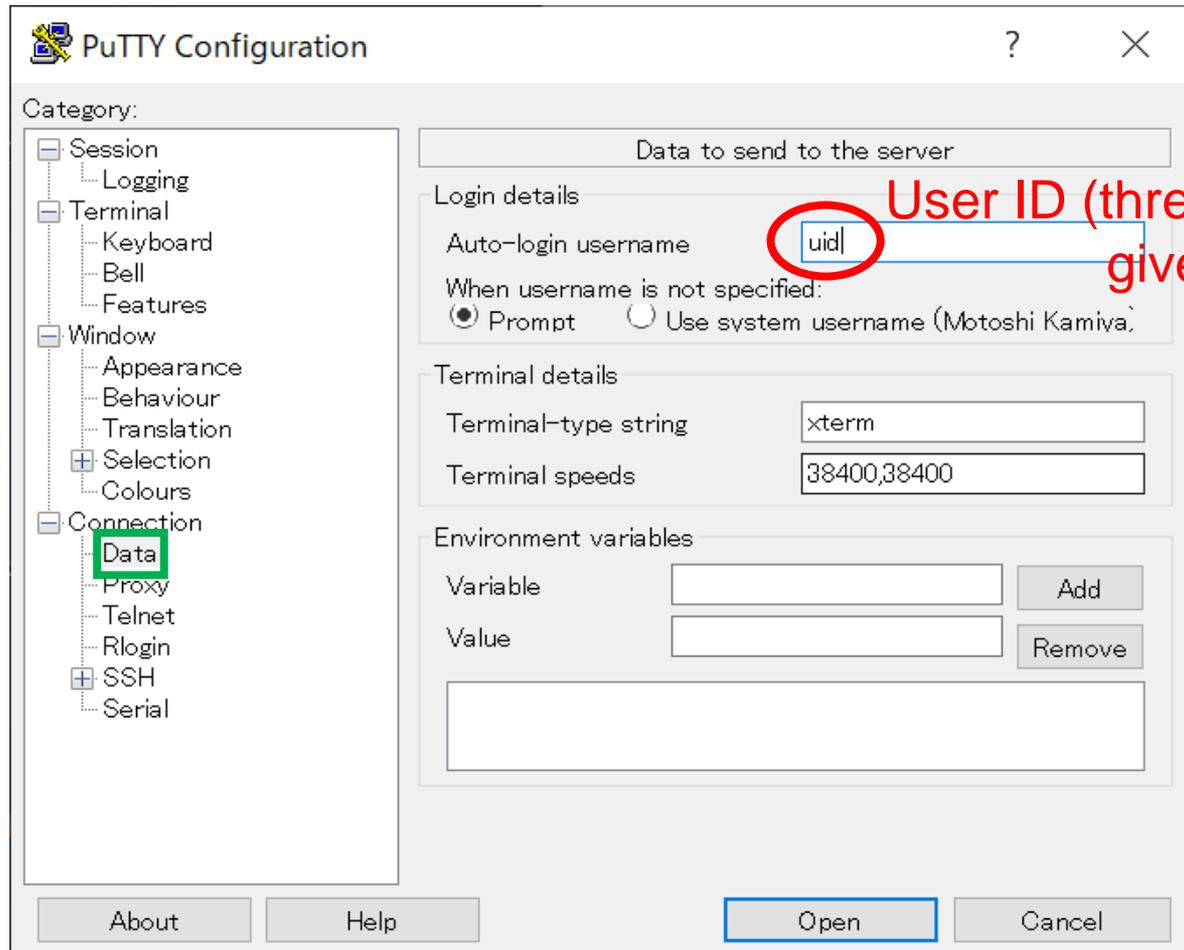
(This step can be skipped. In that case, you will be asked upon connection.)

Login (4)

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

Login (5)

Move to [Session], save settings, and then login.
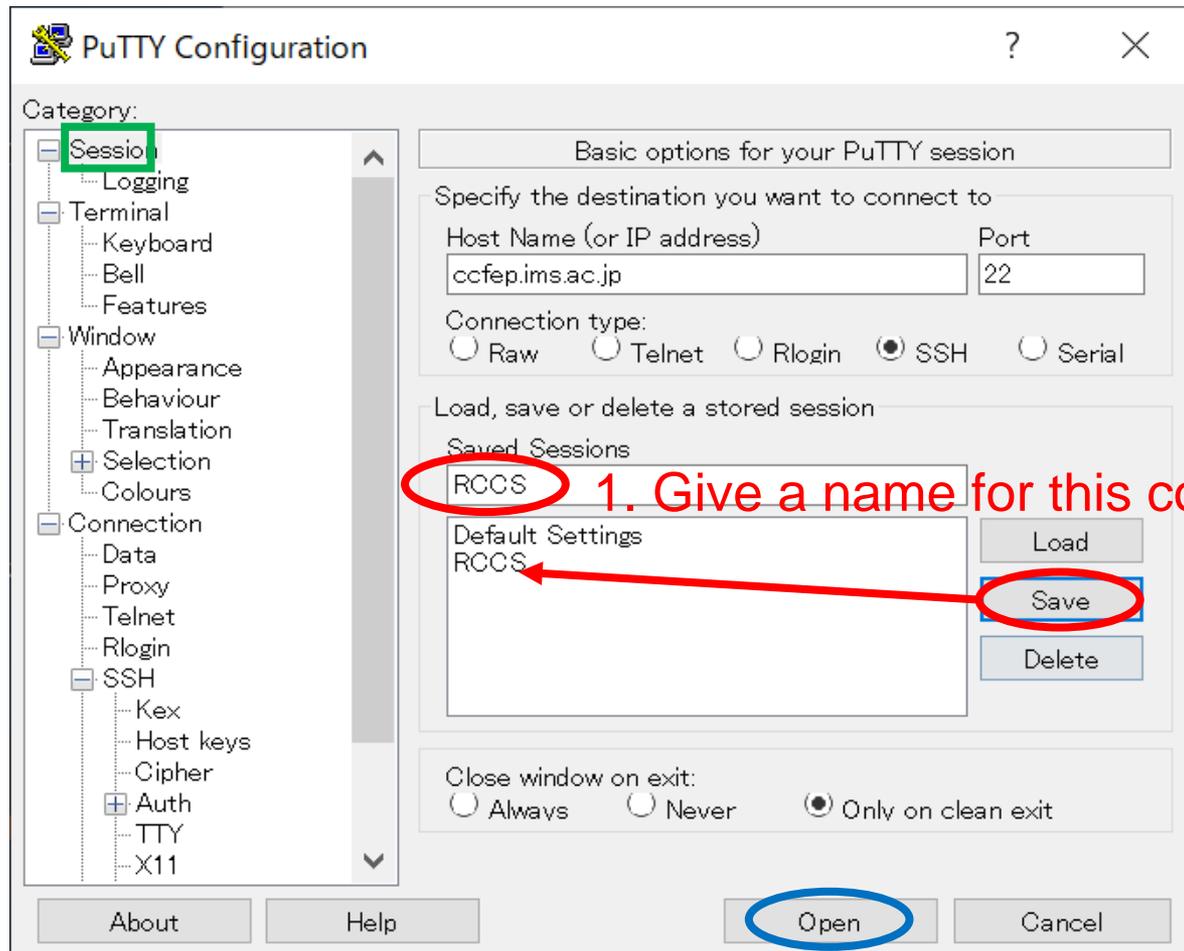
1. Give a name for this connection

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.

[はい(Y)] [いいえ(N)] [キャンセル] [ヘルプ]

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

2. 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/DdGr2PlNeoivFRR8v5krXHEmdU (SHA256)
- 0KL38Yn/kBee1pAuxyKwenEwXjtPxr9ZEloIfVqXvbI (SHA256)
- Nhg+9Lgj3XeuW//A/j7jqgUJlIxWehryCtStIp1Dirs (SHA256)

Login (7)

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

Login (8)

Once you types correct passphrase, login to RCCS frontend server will be granted.
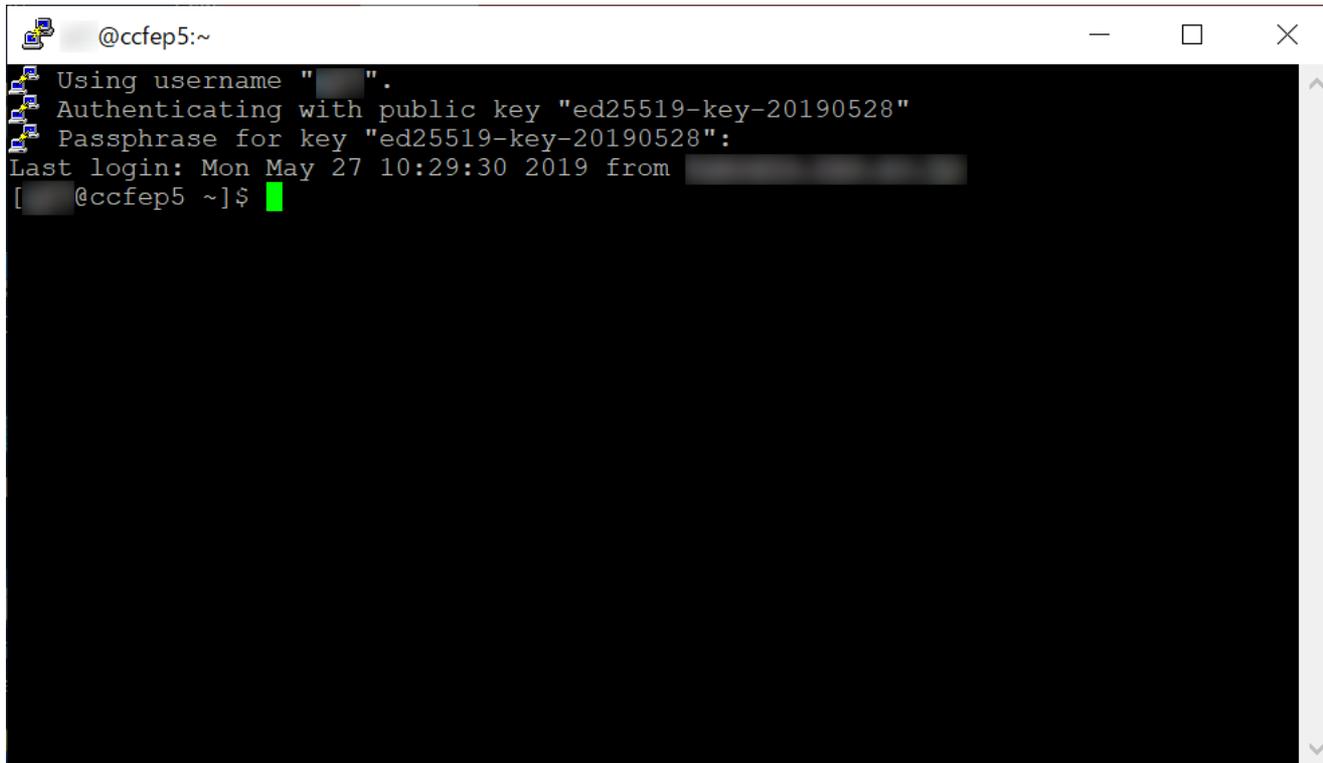
Note: if you launch Pageant and your key is registered, passphrase won't be asked upon connection. (You need to type passphrase upon registration to Pageant.)