

SSH key creation and login (PuTTY version)

National Institutes of Natural Sciences
Okazaki Research Facilities
Research Center for Computational Science (RCCS)

(Confirmed with PuTTY 0.75)

Changelog

- Jul 10, 2019 First version
- Feb 2, 2021 Update (recommended key types etc.)
- May 24, 2021 Update for PuTTY 0.75

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.)

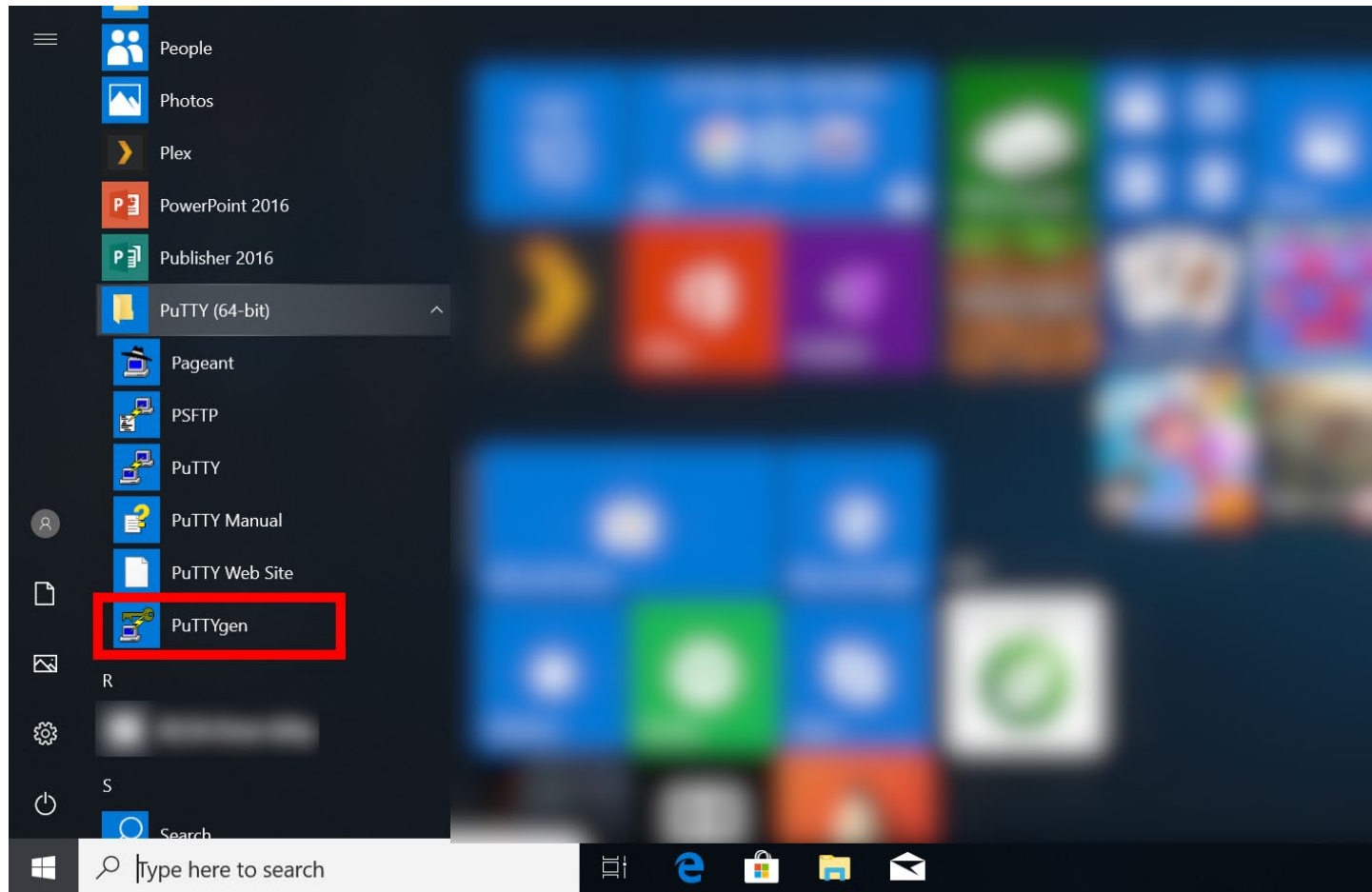
MSI (Windows Installer) version is recommended.

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.



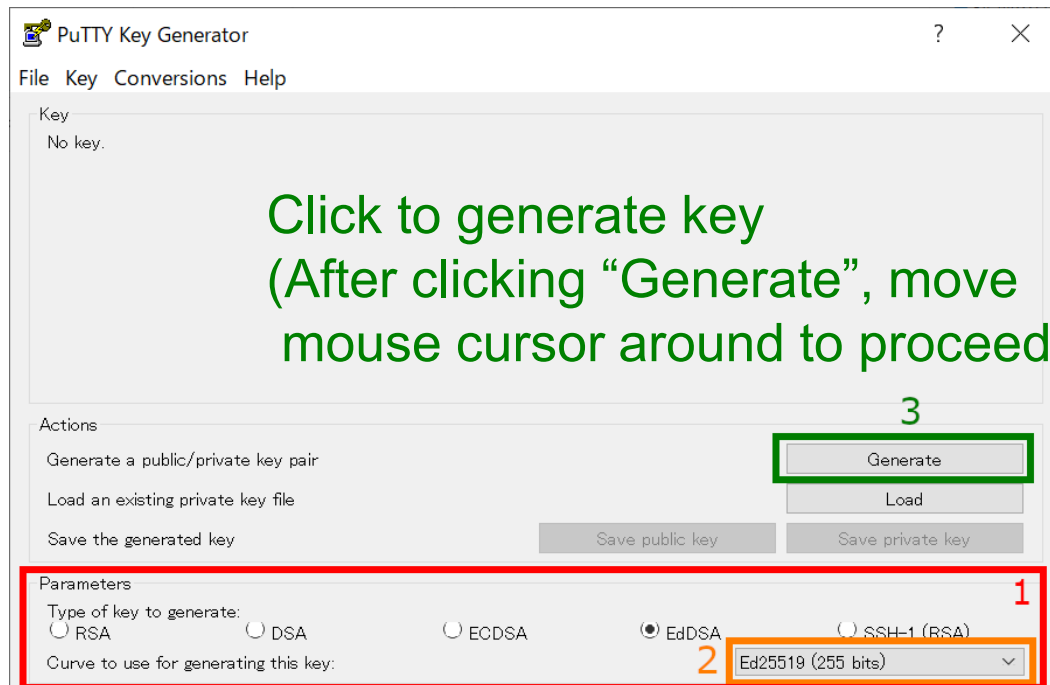
SSH key creation (2)

RCCS recommends following types of keys.

- 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!
Frontend servers don't support that!

Choose Ed25519 if you have no preference.

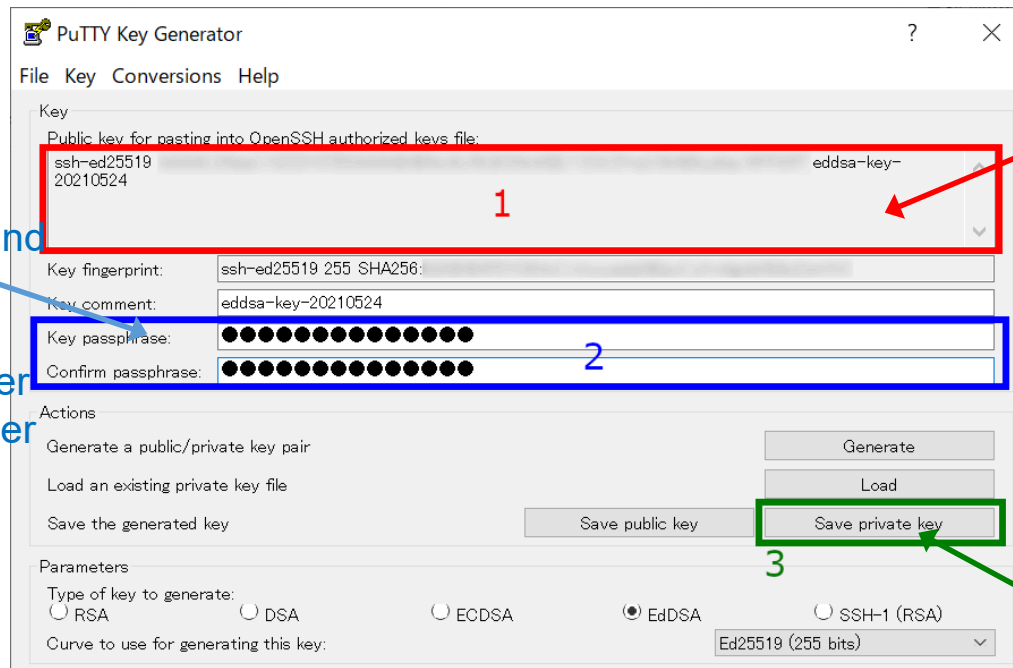


Select key type

Choose key length (RSA, ECDSA, EdDSA)

SSH key creation (3)

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



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 ccfepp.ppk.

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

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

- 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.

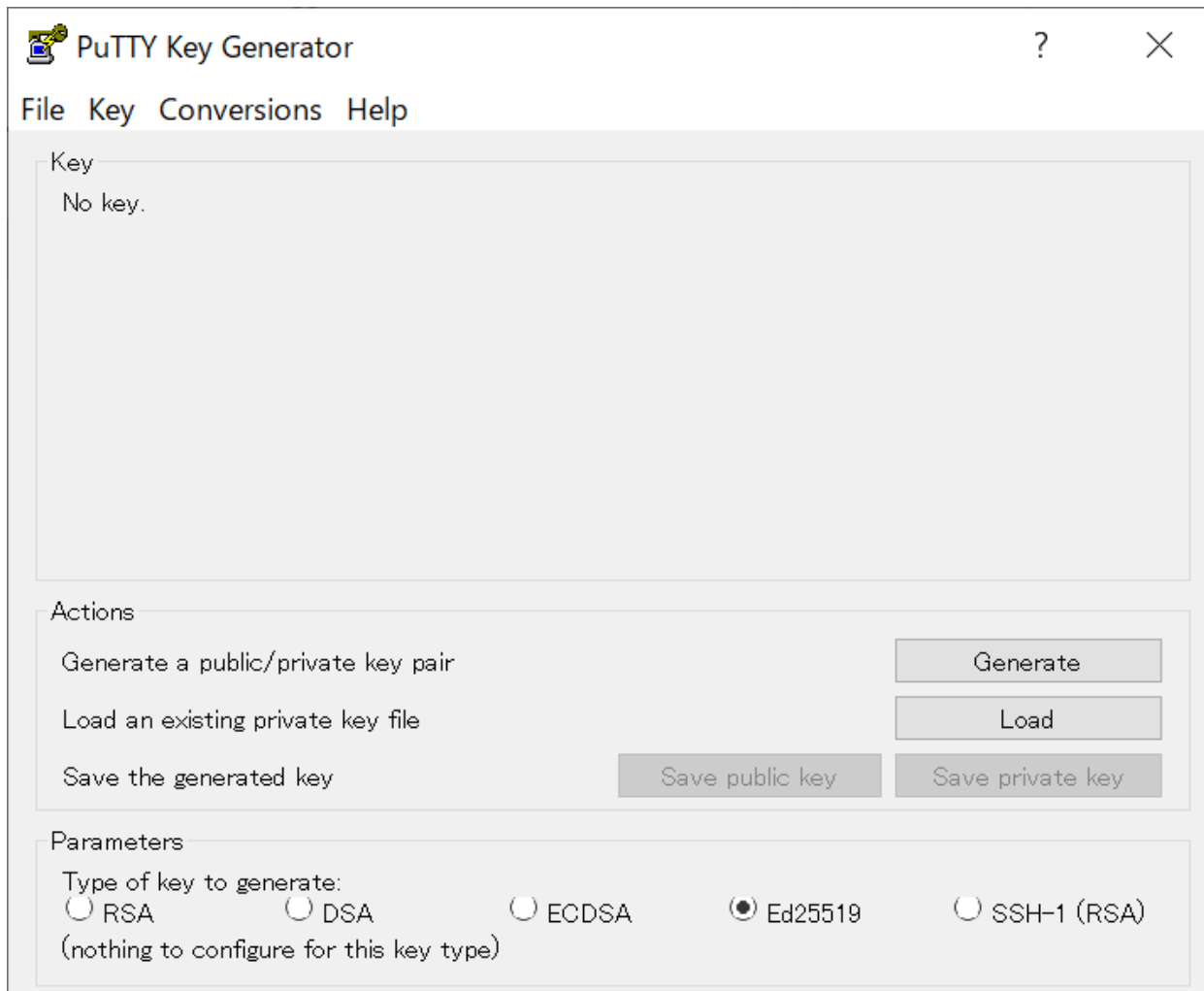
<https://ccportal.ims.ac.jp/en/account/>

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.

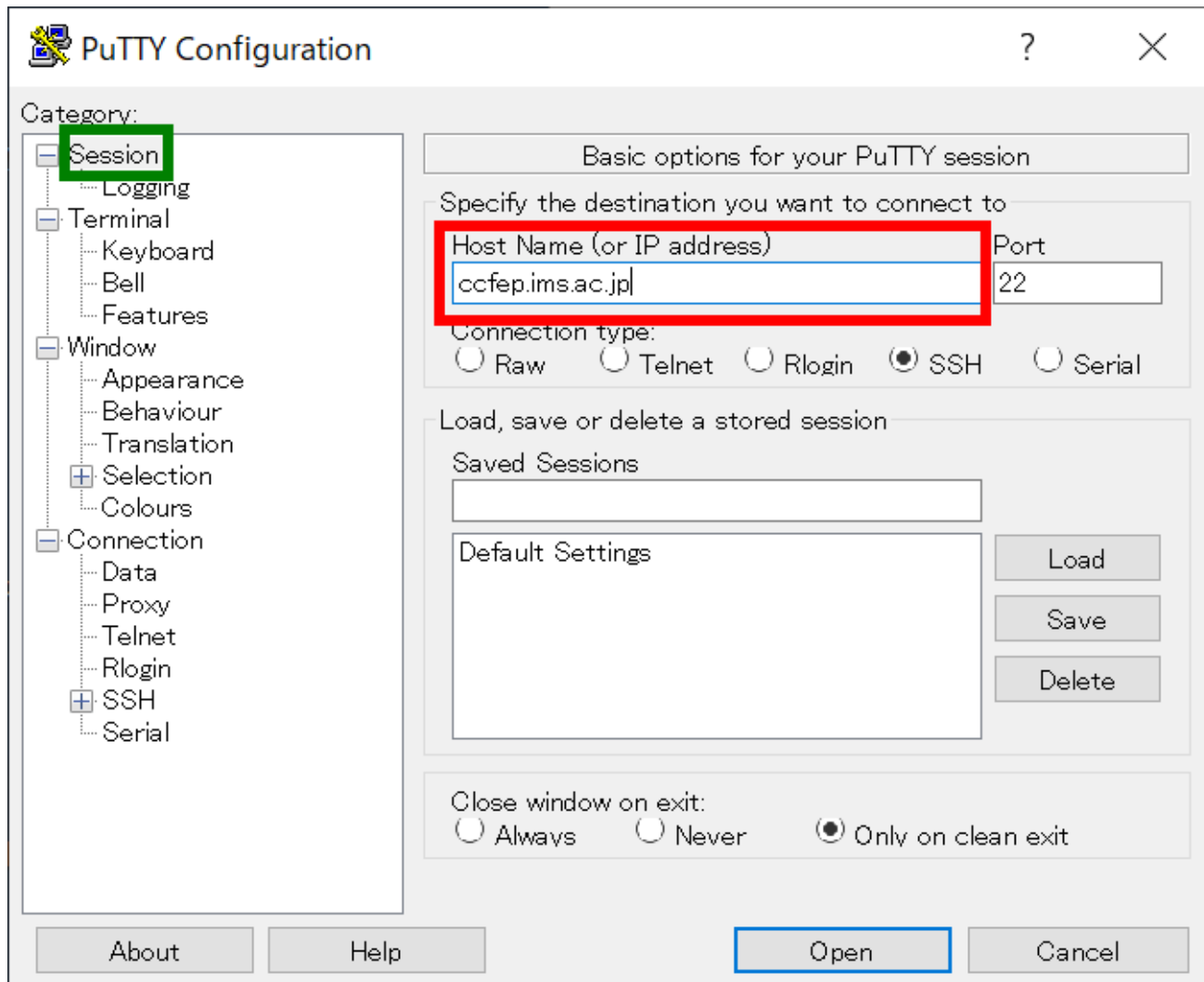
Login (1)

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



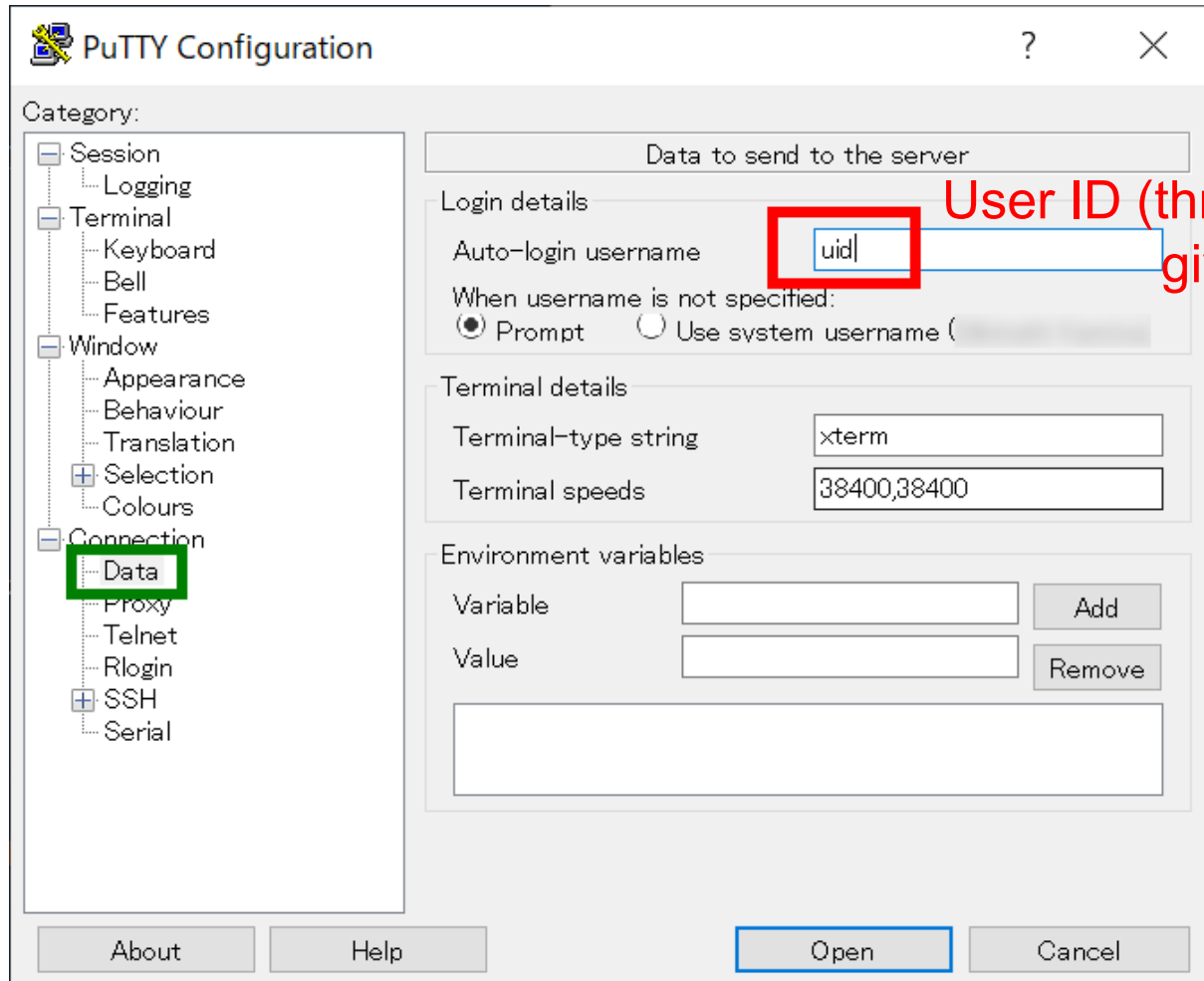
Login (2)

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



Login (3)

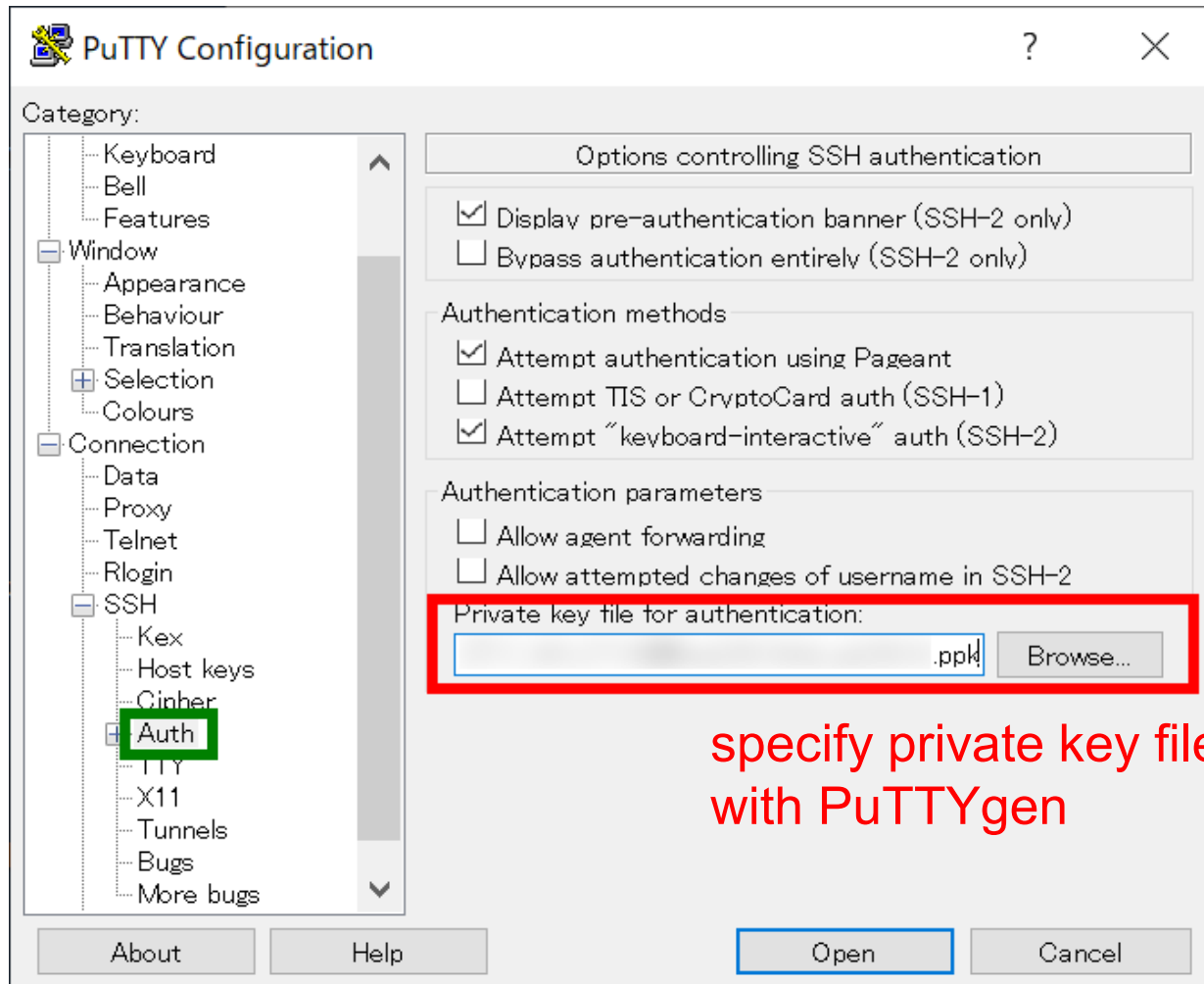
Move to [Connection] -> [Data] and fill your ID in the username box.



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

Login (4)

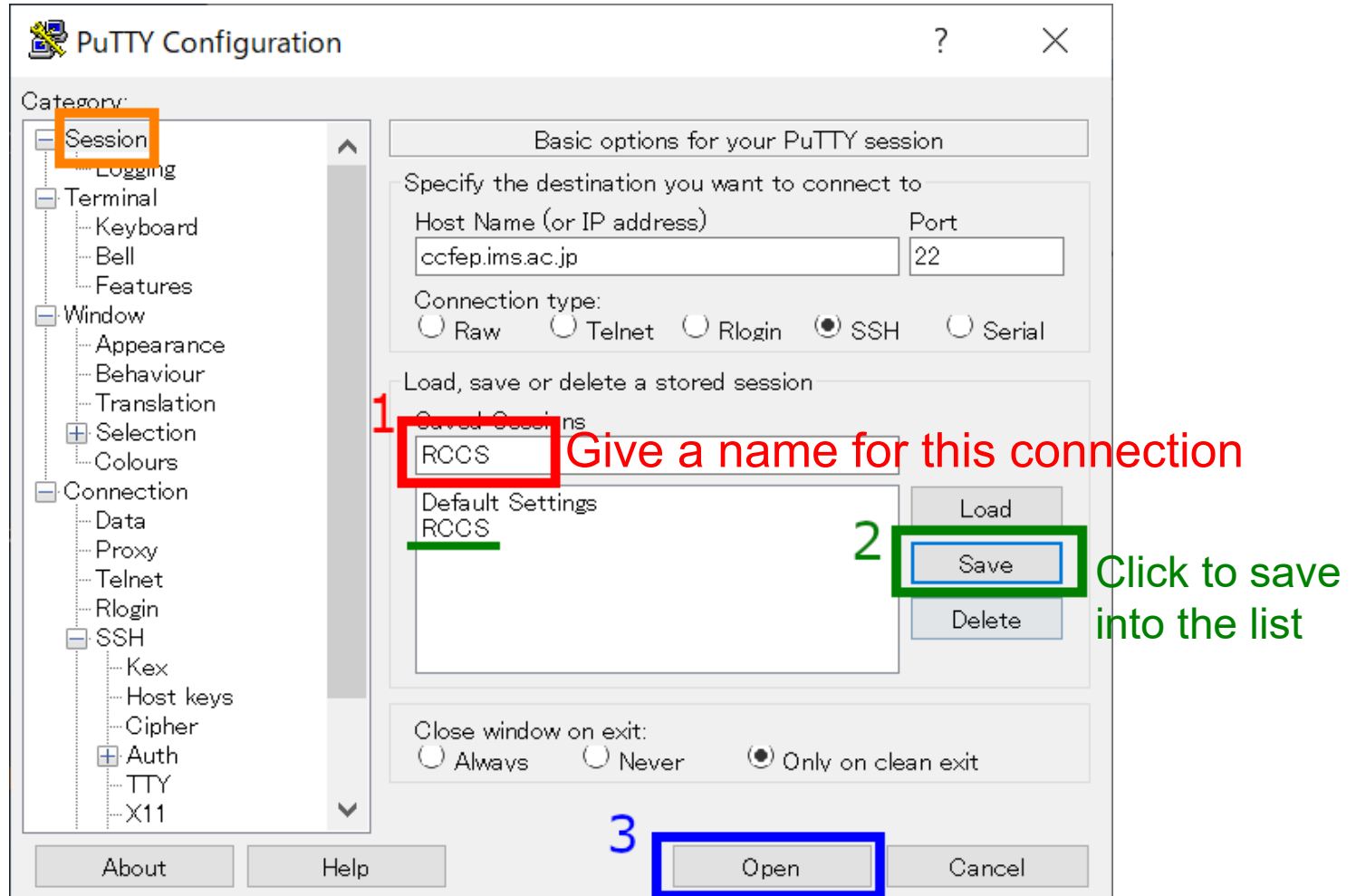
Move to [Connection] -> [Data] -> [SSH] and specify private key (.ppk file)



specify private key file generated with PuTTYgen

Login (5)

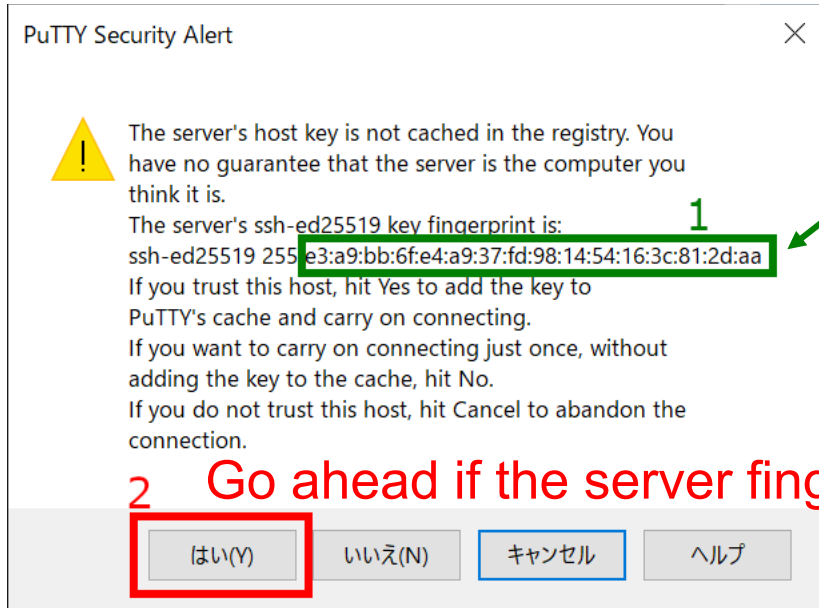
Move to [Session], save settings, and then login.



Let's login!

Login (6)

Upon first connection, alert message will be shown.



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/DdGr2PINeoivFRR8v5krXHEmdU (SHA256)
- 0KL38Yn/kBee1pAuxyKwenEwXjtPxr9ZElolfVqXvbl (SHA256)
- Nhg+9Lgj3XeuW///A/j7jqgUJllxWehryCtStlp1Dirs (SHA256)

Login (7)

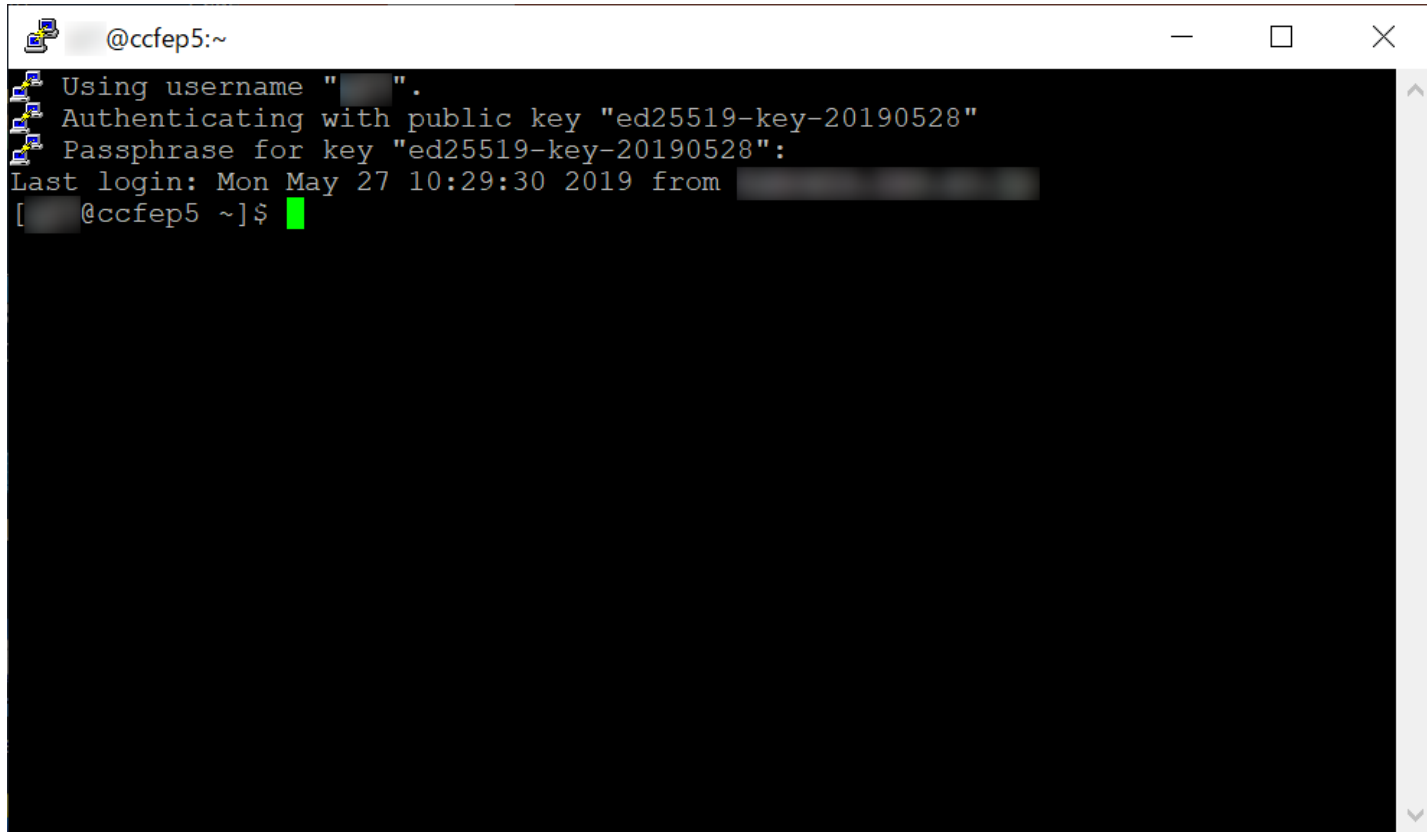
You will be asked passphrase of private key. Type it.



```
ccfep.center.ims.ac.jp - PuTTY
Using username " ".
Authenticating with public key "ed25519-key-20190528"
Passphrase for key "ed25519-key-20190528": █
```


Login (8)

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

A terminal window titled "@ccfep5:~" showing the output of an SSH connection. The text displayed is: "Using username "[REDACTED]".", "Authenticating with public key "ed25519-key-20190528"", "Passphrase for key "ed25519-key-20190528":", and "Last login: Mon May 27 10:29:30 2019 from [REDACTED]". The prompt "[REDACTED]@ccfep5 ~]\$" is followed by a green cursor.

```
@ccfep5:~  
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.)