SSH Key Creation and Login (Tera Term version)

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

(Confirmed with Tera Term 4.105 (SVN# 8433))

Changelog

- Jul. 11, 2019 First version
- Jan. 15, 2020 Minor update of images for version 4.105
- Feb 2, 2021 Minor updates including recommended key types

Introduction

The aim of this document is to explain how to login to RCCS supercomputer using Tera Term.

Table of Contents

Install Tera Term

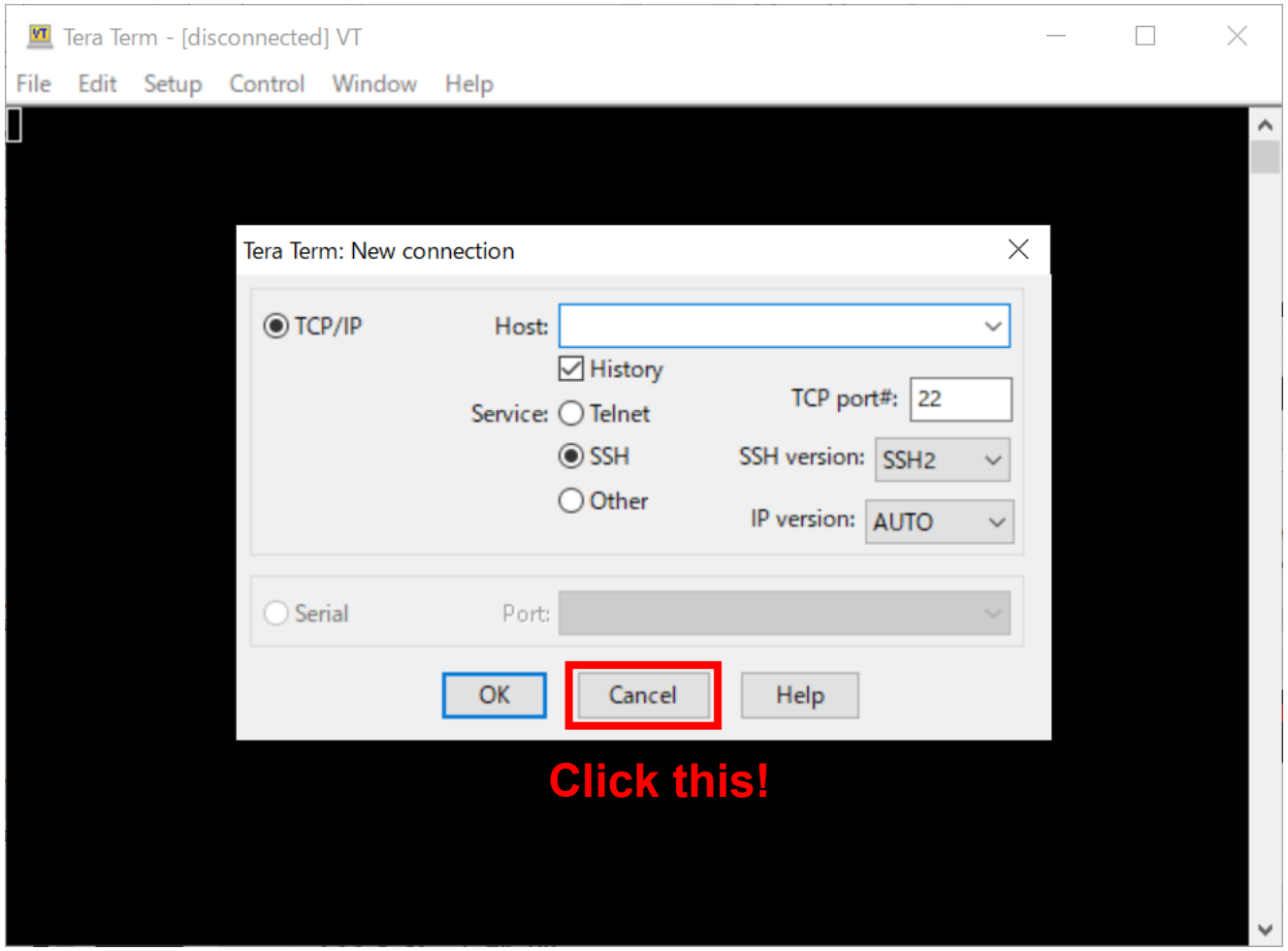
Tera Term can be downloaded from the following site.

https://osdn.net/projects/ttssh2/releases/

Please install Tera Term according to the instruction.

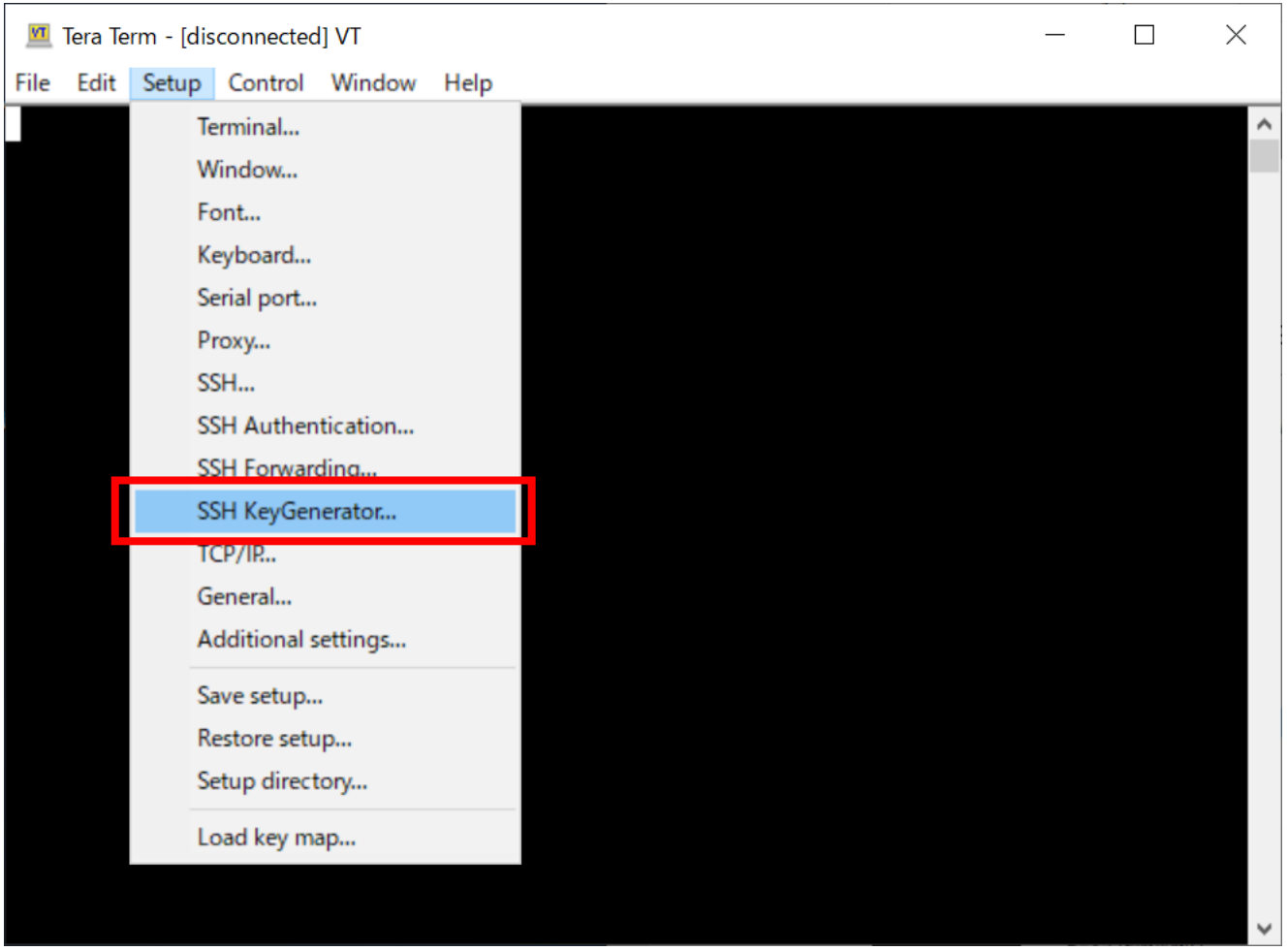
SSH key creation (1)

Launch Tera Term, and then cancel connection.



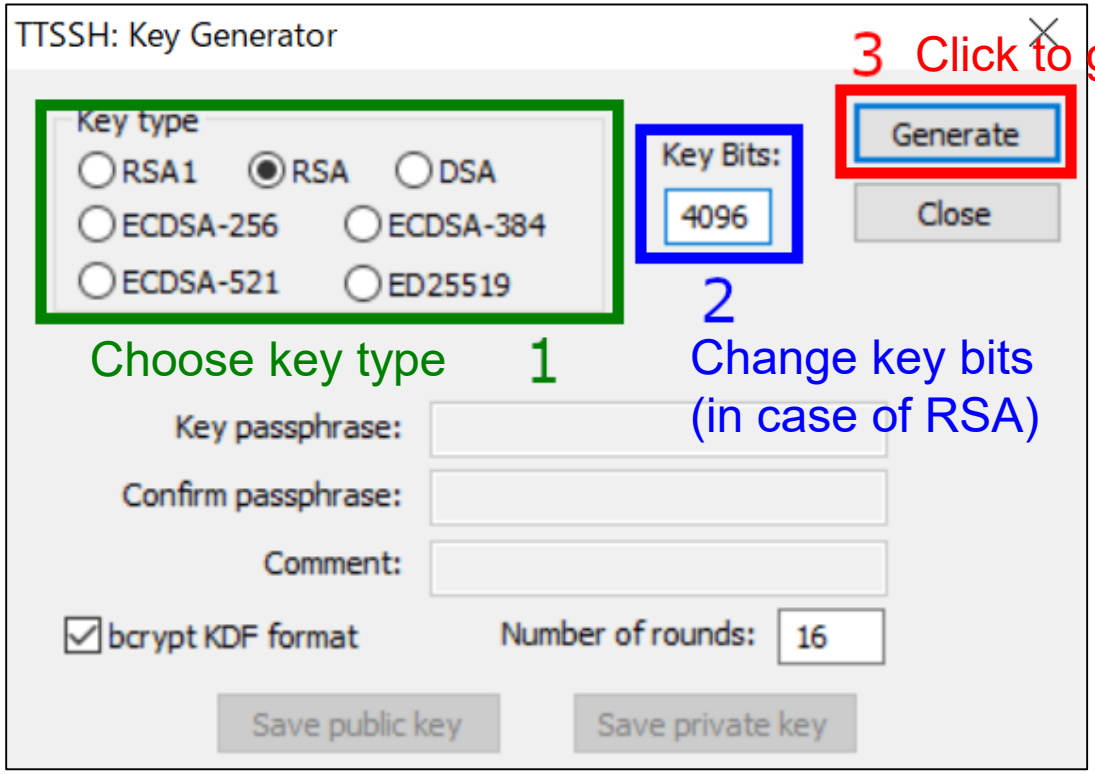
SSH key creation (2)

Select [SSH KeyGenerator] from [Setup] menu.



SSH key creation (3)

Specify key type and the click “Generate” button.



* SHA2 RSA algorithms (rsa-sha2-256/512) are not yet supported in TeraTerm 4.105 (will be avail in 4.106).
If SHA1 algorithm (ssh-rsa) is disabled, it may cause trouble upon RSA authentication.
Note: SHA1 and SHA2 use the same key type. You usually don’t need to generate key again upon migration to SHA2.

Following key types are recommended in RCCS:

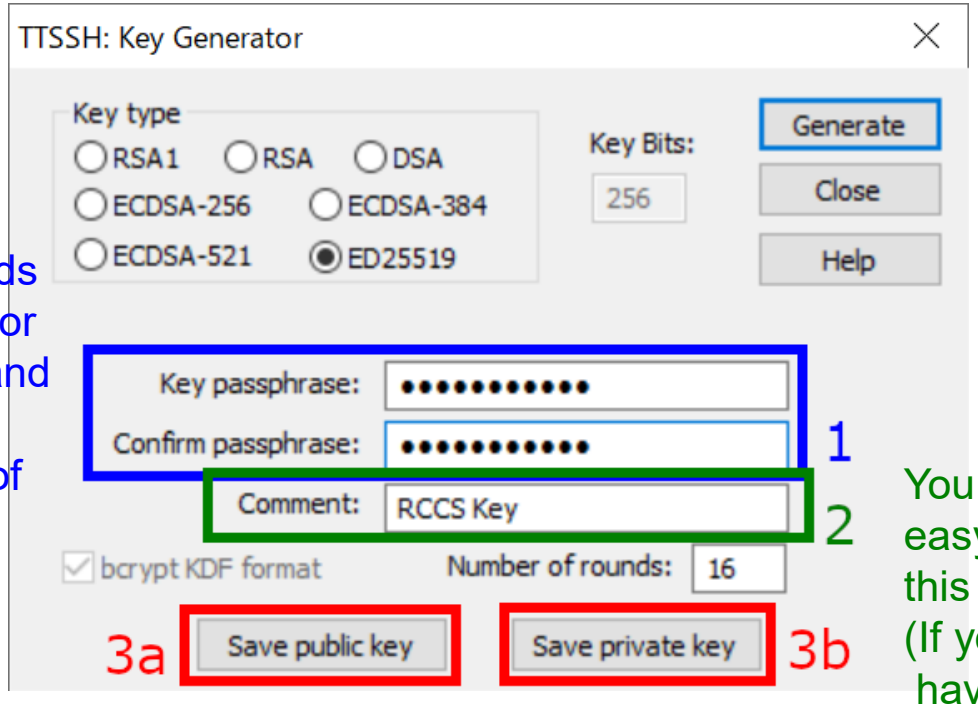
- ED25519
- ECDSA-521, ECDSA-384, ECDSA-256
- RSA 4096 bits (choose RSA and change “Key bits” to 4096)*

If you have no preference, try ED25519.

SSH key creation (4)

Once key generation finished, set passphrase and then save both of two keys (public key & private key)

RCCS recommends passphrase of 10 or more characters and containing all the following 4 types of characters.
- Lower case
- Upper case
- Number
- Symbol



save public key

save private key

You might want to give an easy-to-understand name for this key.
(If you don't have any plans to have other SSH keys, default name would be enough.)

The private key file must be kept secret!

Register Public Key

Before login, you need to register the public key.

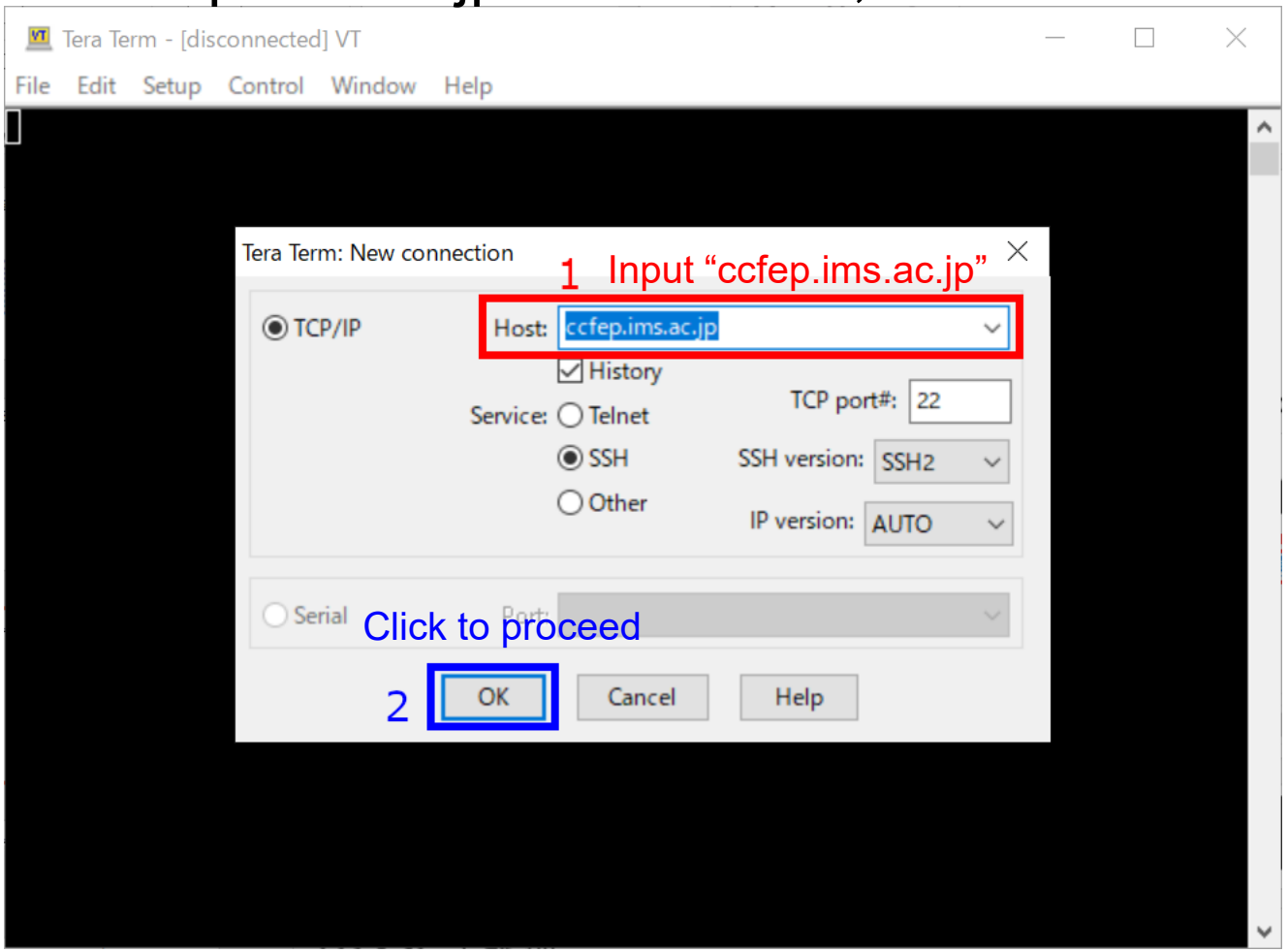
The procedure of the public key registration is available from the following link.
https://ccportal.ims.ac.jp/en/account/

The private key file must be kept secret.

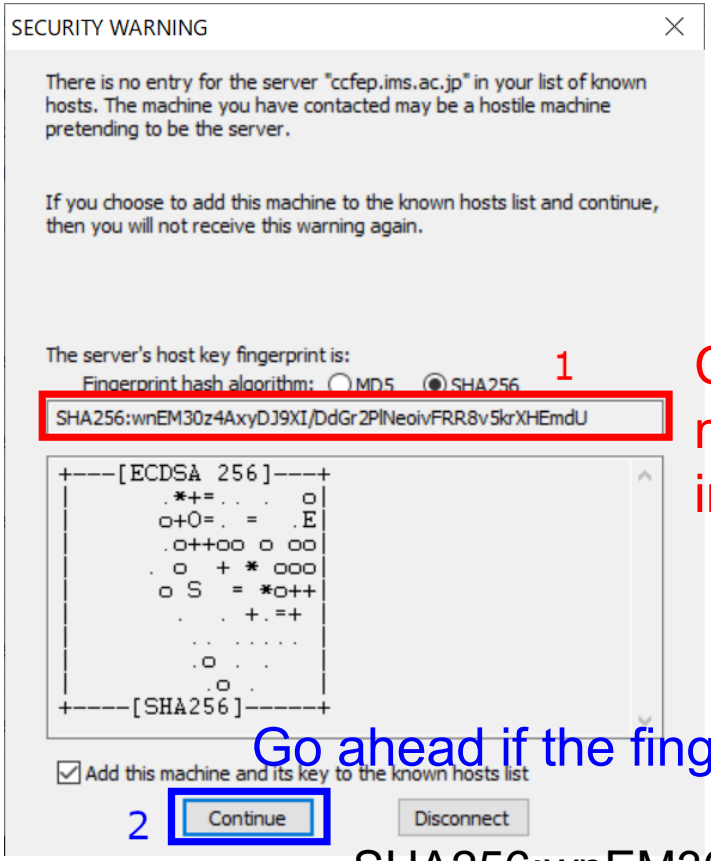
Login (1)

Restart Tera Term or select [New connection] from [File] menu to go back to the initial state.

Then type “ccfep.ims.ac.jp” in Host box, and click “OK”.



Login (2)



Upon first connection, security alert will be shown.

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

Go ahead if the fingerprint is valid

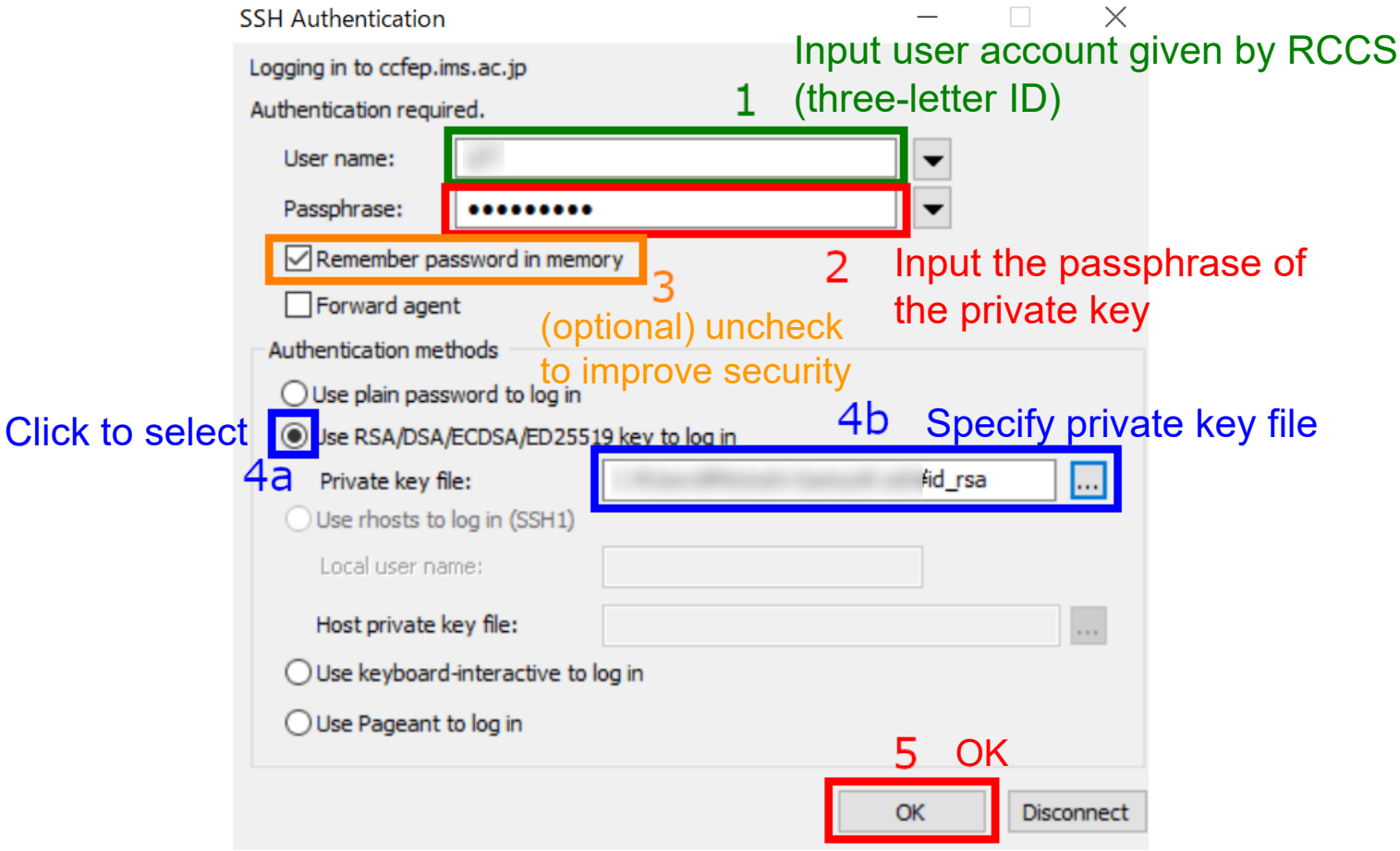
Fingerprints of valid server keys

- SHA256:wnEM30z4AxyDJ9XI/DdGr2PlNeoivFRR8v5krXHEmdU
- SHA256:0KL38Yn/kBee1pAuxyKwenEwXjtPxr9ZElolfVqXvbI
- SHA256:Nhg+9Lgj3XeuW//A/j7jqgUJlIxWehryCtStIp1Dirs

- MD5: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

Login (3)

Input your ID, private key location, and passphrase for the private key.



(You can set default user name and private key location on “Setup” menu.)

Login (4)

If everything works fine, you will successfully login to frontend.