# 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)



• 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

1. Select key type

Use RSA 4096 if you have no preference.

PuTTY Key Generator		? ×	
File Key Conversions Help			
Key No key.			
Actions		2. Click t	o generate key
Generate a public/private key pair Load an existing private key file Save the generated key	Save public ke	Generate Load Save private key	
Parameters Type of key to generate: ● RSA ○ DSA Number of bits in a generated key:	⊖ ecdsa → ed25	5519 () <u>SCU 4 (DSA)</u> 4096	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	PuTTY Key Generator File Key Conversions Help Key Public key for pasting into OpenSSH authorized_keys file:			? ×	<ol> <li>This is the public key we need. You should save this key in a file.</li> <li>(Please copy whole the</li> </ol>		
or more characters and containing all the following 4 types of characters.	Key fingerprint: Key comment: Key passphrase: Confirm passphrase: Actions	ssh-rsa 4096 rsa-key-20190528 ••••••			key. This window is often too small for sor types of keys.)		
<ul> <li>lower-case character</li> <li>upper-case character</li> <li>number</li> <li>symbol</li> </ul>	Generate a public/priv Load an existing priva Save the generated ke Parameters Type of key to genera (• RSA () Number of bits in a ge	vate key pair te key file ay Sa te: DSA OECDSA nerated key:	ve public key Sav	Generate Load re privatetkey ) SSH-1 (RSA) 096	3. Click to save the private key. You might want to choose easy-to-understand filename such as		

- 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.

👺 PuTTY Configuration		?	$\times$
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 see Specify the destination you want to connect Host Name (or IP address) Connection type: Raw Telnet Rlogin SSH Load, save or delete a stored session Saved Sessions Default Settings Close window on exit: Always Never Only on cl	ean exit	ial
About Help	Open	Cance	

## 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 Translation Colours Connection Data Proxy Telnet Rlogin Serial	Basic options for your PuTTY session         Specify the destination you want to connect to         Host Name (or IP address)       Port         ccfep.ims.ac.jp       22         Connection type:       22         Raw       Telnet       Rlogin       SSH         Load, save or delete a stored session       Saved         Default Settings       Load         Save       Delete         Close window on exit:       Image: Only on clean exit
About Help	Open Cancel

# Login (3)

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

😹 PuTTY Configuration		?	$\times$	
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Serial	Data to send to the server Login details Auto-login username When username is not specified: Prompt Use system username (N Terminal details Terminal-type string xterm Terminal speeds 38400,38400 Environment variables Variable Value	votoshi k	D (thr giv (amiva) Add emove	ee letter ID ven by RCCS)
About Help	Open	Ca	incel	

(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.

Butty Configuration		?	$\times$	
Category:				
<ul> <li>Logging</li> <li>Terminal</li> <li>Keyboard</li> <li>Bell</li> <li>Features</li> <li>Window</li> <li>Appearance</li> <li>Behaviour</li> <li>Translation</li> <li>Selection</li> <li>Colours</li> <li>Connection</li> <li>Data</li> <li>Proxy</li> <li>Telnet</li> <li>Rlogin</li> <li>SSH</li> <li>Kex</li> <li>Host keys</li> <li>Cipher</li> </ul>	Specify the destination you want to connect Host Name (or IP address) [ccfep.ims.ac.jp Connection type: () Raw () Telnet () Rlogin () SS Load, save or delete a stored session Saved Sessions RCCS 1. Give a name Default Settings RCCS	Port 22 SH O Se for th Load Save Delet		onnection 2. Click to save into the list
	◯ Alwavs ◯ Never (● Only on	clean exit		
About Help	Open	Cano	el	

3. Let's login!



Upon first connection, alert message will be shown.



- 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)
   of valid
   wnEM30z4AxyDJ9XI/DdGr2PINeoivFRR8v5krXHEmdU (SHA256)
  - 0KL38Yn/kBee1pAuxyKwenEwXjtPxr9ZElolfVqXvbI (SHA256)
  - Nhg+9Lgj3XeuW//A/j7jqgUJIIxWehryCtStIp1Dirs (SHA256)



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





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.)