



AI Bridging Cloud Infrastructure “ABCI” Tutorial (Preparation)

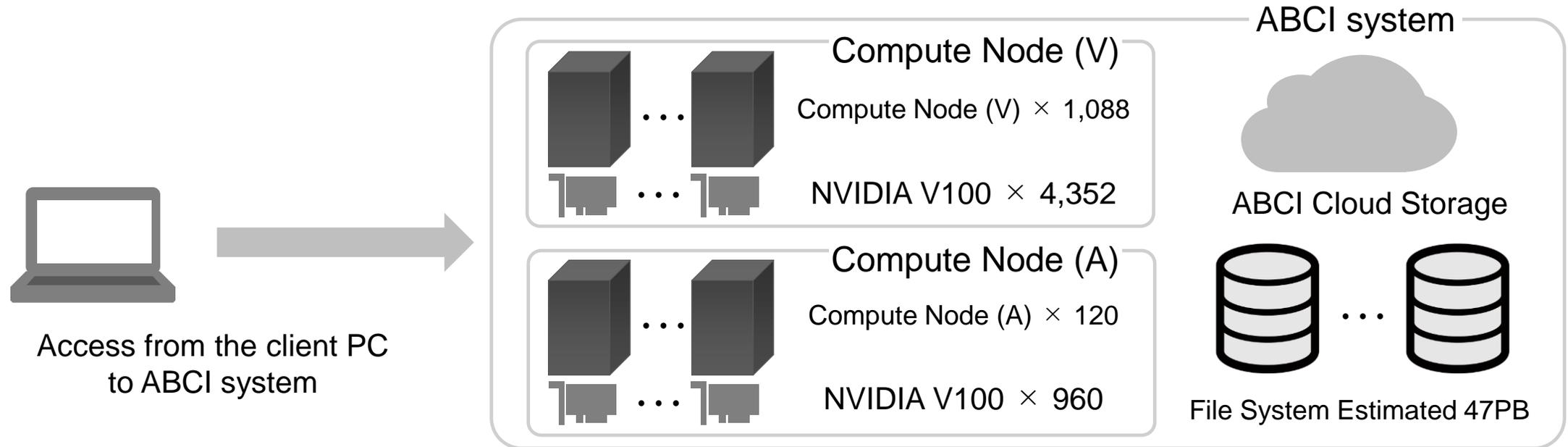
Digital Architecture Promotion Center

Department of Information Technology and Human Factors
National Institute of Advanced Industrial Science and Technology

CONTENTS

- Setup Client PC Environment
 - Windows: Using Windows Subsystem for Linux
- ABCI System Usage Procedure
(Assuming you have already applied for and obtained an account)
 - Access to the User Portal
 - Initial Login
 - Declaration for the Applicability of the Specific Categories
 - Features
- Generate public and private key pairs
 - Key generation with commands from Terminal
 - Key generation with PuTTYgen
 - To convert keys generated by another tools for PuTTY
- Register a public key
- Log in to the ABCI system
 - Log in from Terminal
 - Using PuTTY
- Reference Links Summary

Setup Client PC Environment



The ABCI system consists of the following hardware and software.

- 1,088 nodes of Compute Nodes (V) with a total of 4,352 NVIDIA V100 GPU accelerators
- 120 nodes of Compute Nodes (A) with a total of 960 NVIDIA A100 GPU accelerators
- Approximately 47 PB of shared file system and ABCI cloud storage

Linux-based operating systems are used for these Compute nodes.

To run jobs on the Compute Nodes of the ABCI system, users access them via an access server.

Setup Client PC Environment - In case of Windows PC -

Using Windows Subsystem for Linux (WSL) to build an environment that runs Linux on Windows

WSL is a mechanism to run a Linux environment on Windows, allowing Linux commands and applications to run on Windows. However, since the installation procedure differs depending on the Windows version, please update your Windows to the latest version before installing WSL.

Please refer to the "Reference Links" below for detailed procedures. The main procedure is as follows.

(Tip: Some BIOS settings may be required depending on your PC to use the virtual machine functionality.)

1. Enable Windows subsystem for Linux.
2. Enable the "Virtual Machine Platform (Hyper-V)" optional feature.
3. Download and install Linux kernel package.
4. Download and install Ubuntu.

Reference Links:

- https://qiita.com/boss_ape/items/6f1e1f731b5385f4b31a
- <https://qiita.com/fumikomatsu/items/01e5cfa09347176f4d1a>
- <https://chigusa-web.com/blog/wsl2-win11/>

ABCI System Usage Procedure

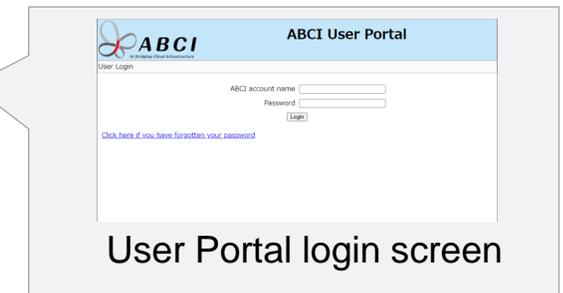
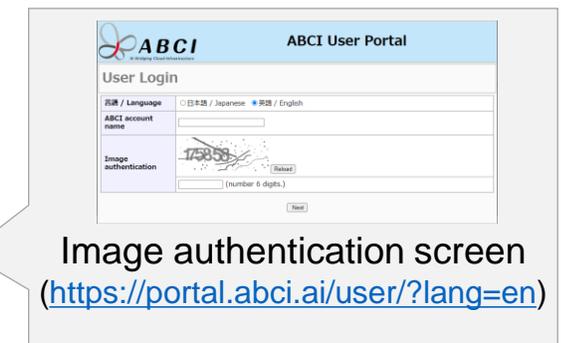
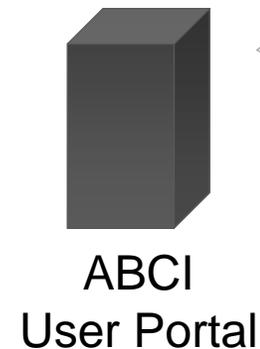
- Access to the User Portal -

Access to the “ABCI User Portal”, which manages various information in using the ABCI system, to register, manage, and check necessary information.

The “ABCI User Portal” is a site that manages information required to use the ABCI System. Before using the ABCI system, access the “ABCI User Portal” to register and confirm necessary information. After accessing the “ABCI User Portal” and completing the necessary procedures, you will receive an e-mail with a login URL.



- ① Access the “ABCI User Portal” with a browser.
- ② Enter your account name and pass the image authentication.
- ③ The login URL will be sent to the registered e-mail address.
- ④ Access the login URL in the e-mail sent to you.
- ⑤ Enter your ABCI system account name and password to log in.



ABCI System Usage Procedure

- Initial login to the User Portal -

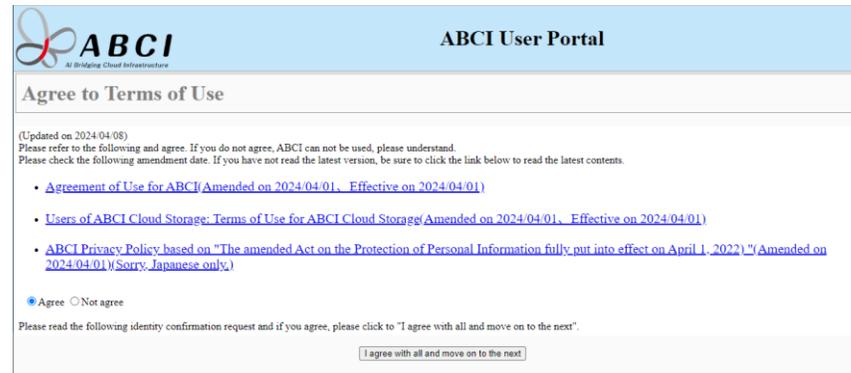
When you log in to the User Portal for the first time, agree to the Terms of Use and change from a temporary password.

– Initial login to the User Portal –

When you register to use the ABCI system, you will receive an e-mail containing your initial login URL, temporary password, and account. Please access the "User Portal" from the URL for initial login, agree to the Terms of Use, and change the temporary password.



① Access URL for initial login



② Agree to the Terms of Use



③ Change from temporary password

Reference: [ABCI Portal Guide - 2. User Portal](#)

ABCI System Usage Procedure

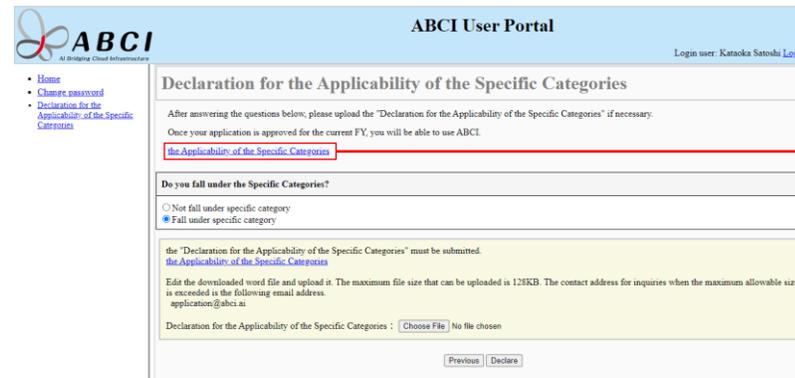
- Declaration for the Applicability of the Specific Categories -

When you log in to the User Portal for the first time in each fiscal year, please complete the “Declaration for the Applicability of Specific Categories”.

- When logging in to the “User Portal” for the first time in each fiscal year – You will receive two E-mails containing a special password and the URL of the website for “Declaration for the Applicability of Specific Category”.
- Please access to the “User Portal” from the URL for declaration, log in with the temporary password sent to you, and answer the questions displayed.



① Access to the URL for declaration



② Declaration for the Applicability of Specific Categories



- Read the description of the “Applicability for the Specific Categories” and confirm whether you fall under the category or not.

Reference: [ABCI Portal Guide – 2.1.1 Declaration for the Applicability of Specific Categories](#)

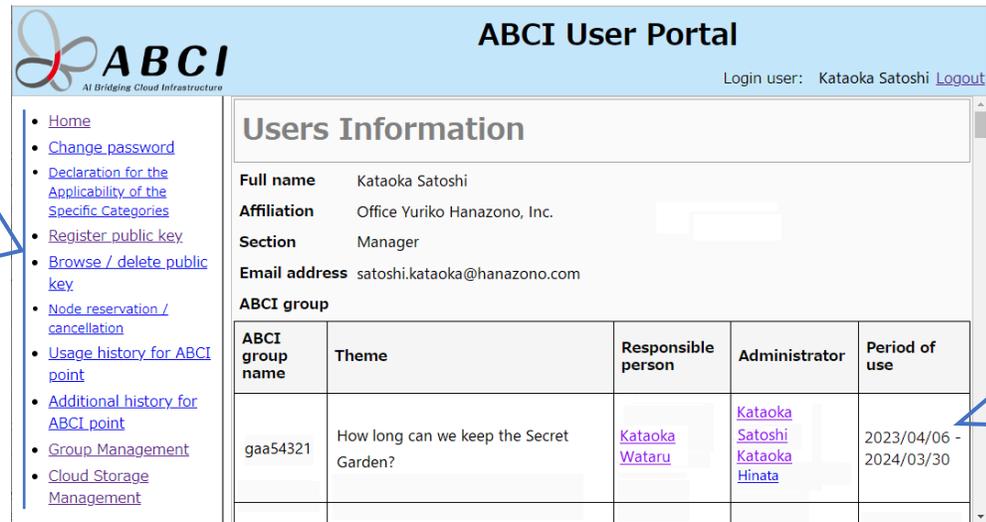
ABCI System Usage Procedure

- User Portal: Features -

The "ABCI User Portal" allows you to manage users of the ABCI system, add points, check history of additional/usage point, and register public keys to connect to the ABCI system.

Upon logging in to the ABCI User Portal, you can view and manage information necessary for using the ABCI system. For details on each function, please refer to "ABCI Portal Guide: 2. User Portal, 3. User Administrator Authority".

- [Users]
- Change / Reissue password
 - Register / Browse / Delete public key
 - List of Node reservation / cancellation
 - Usage History for ABCI Point
 - Cloud Storage Management
- [Requires Supervisory User or User Administrator privileges]
- Node reservation / cancellation
 - Details of Usage History for ABCI Point
 - Additional history for ABCI point additions
 - Group Management
 - Cloud Storage Management



The screenshot shows the ABCI User Portal interface. The top header includes the ABCI logo and the text "ABCI User Portal". The user is logged in as "Kataoka Satoshi" with a "Logout" link. The main content area is titled "Users Information" and displays the following details:

- Full name:** Kataoka Satoshi
- Affiliation:** Office Yuriko Hanazono, Inc.
- Section:** Manager
- Email address:** satoshi.kataoka@hanazono.com

Below this information is a table titled "ABCI group" with the following columns: ABCI group name, Theme, Responsible person, Administrator, and Period of use.

ABCI group name	Theme	Responsible person	Administrator	Period of use
gaa54321	How long can we keep the Secret Garden?	Kataoka Wataru	Kataoka Satoshi , Kataoka Hinata	2023/04/06 - 2024/03/30

See the groups and group members that you belong to or manage.

(*Screens vary depending on the authority of the person who logged in)

Reference: ABCI Portal Guide - [2. User Portal](#)
[3. User Administrator Authority](#)

Necessary steps to connect to the ABCI system

- Public and private key generation required for SSH public key authentication
- Create tunneling and login by SSH port forwarding

Generation and registration of the "key" necessary for authentication and connection using SSH port forwarding are required to connect to the ABCI system, since the SSH public key authentication method is used.

We will introduce the below two types of these procedures starting on the next page.

- Using a terminal
- Using SSH client software (PuTTY is covered in this content)

It is not necessary to perform both types of procedures.

There are also other methods not introduced here.

Please use them according to your environment.

Generate public and private key pair

- Key generation with commands from Terminal -

Generate a public/private key pair using the "ssh-keygen" command in the terminal for SSH encrypted communication with the ABCI system.

To connect to the ABCI system, you will need an SSH client and a secure public/private key pair.

Available key pairs for ABCI are RSA keys (2048bit or higher), ECDSA keys (256bit, 384bit, or 521bit), and Ed25519 keys.

Example: Generate a public/private key pair with a terminal (Create a 4096-bit RSA key, add a comment with your e-mail address, and create the key in the /.ssh directory)

Substitute where "satoshi.kataoka@hanazono.com" with your own e-mail address.

```

yourpc$ install -m 0700 -d ~/.ssh
yourpc$ cd ~/.ssh
yourpc$ ssh-keygen -t rsa -b 4096 -C "satoshi.kataoka@hanazono.com" -f ~/.ssh/id_rsa
Generating public/private rsa key pair. Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa.
Your public key has been saved in id_rsa.pub.
yourpc$ ls ~/.ssh
id_rsa  id_rsa.pub

```

Make a directory to put key and set permission

Generate key with "ssh-keygen" command

Enter your passphrase (strongly recommended)

Enter the passphrase again (strongly recommended)

Check that public/private keys have been generated

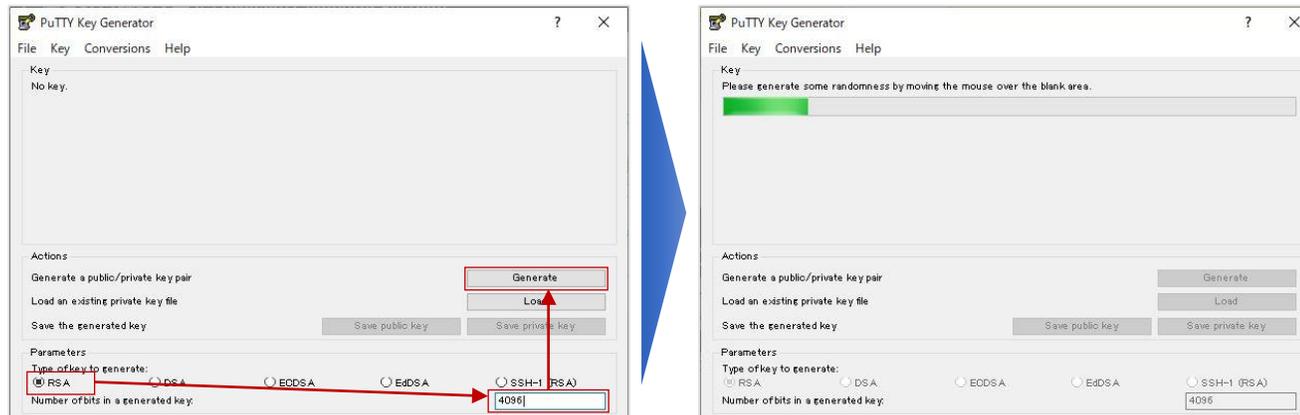
Generate public and private key pairs

- Key generation with PuTTYgen -

Generate public/private keys with "PuTTYgen", a key generation tool for PuTTY

After installing PuTTY, start "PuTTYgen" from the Windows Start menu, and the "PuTTY Key Generator" dialog box will appear. Generate keys from this dialog box. (The version of PuTTY is assumed to be "0.81".)

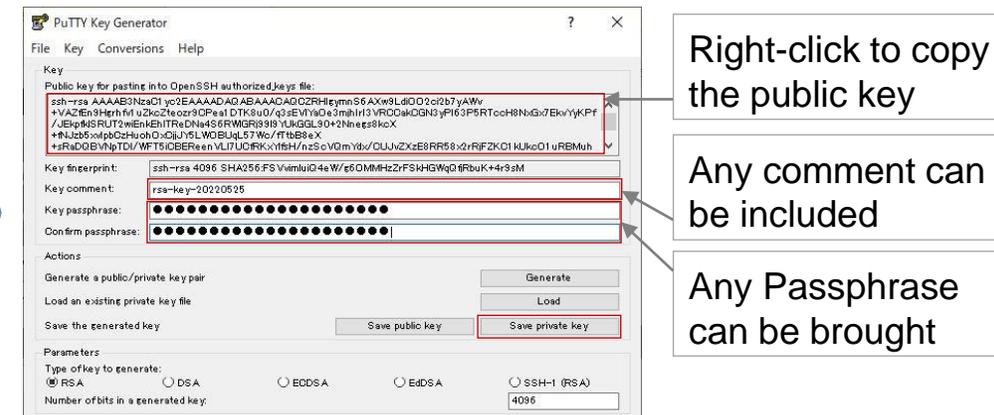
Select the key type and press "Generate".



- For "Parameters", select "RSA", enter "4096" for "Number of bits ...", press "Generate".
(In this example, the key format is the same as in the previous section.)

- Move the mouse until the key generation starts and the green progress bar fills up.

Save the key



Right-click to copy the public key

Any comment can be included

Any Passphrase can be brought

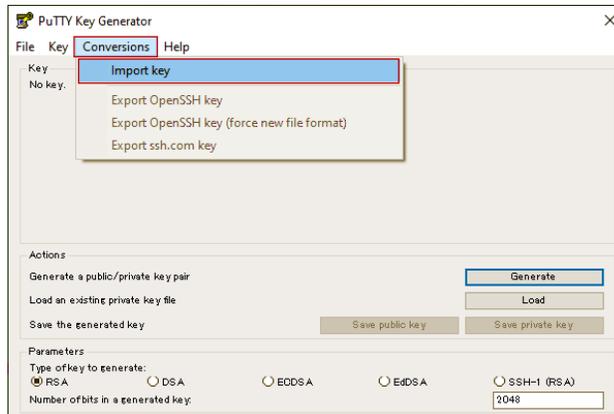
- Enter a comment and passphrase, and press "Save Private Key" to save the private key. Copy the public key by right-clicking with the mouse. (This step is necessary for the public key registration on the next step.)

Generate public and private key pairs

- To convert keys generated by another tools for PuTTY -

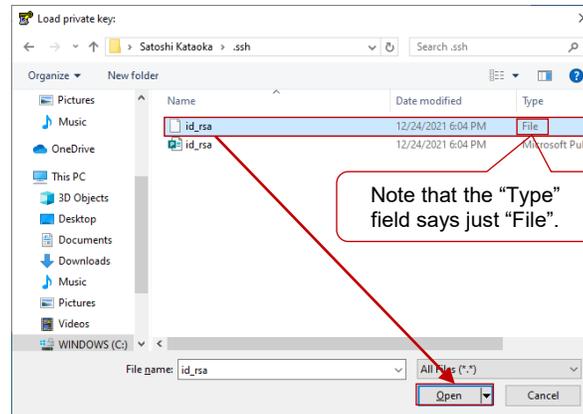
If you have a public/private key generated by another tool and you want to continue to use the public key already registered with the host, you need to convert the private key for PuTTY.

Select the key type and press "Generate".



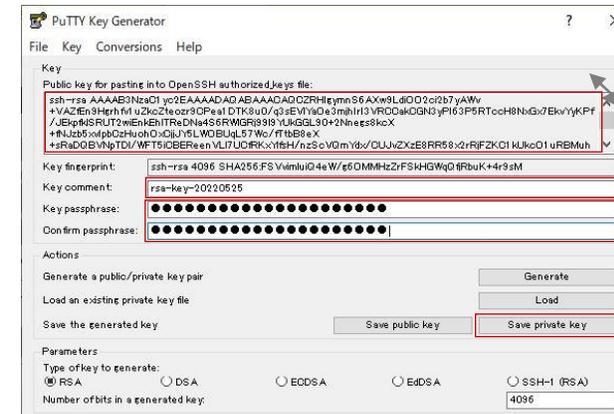
① Launch "PuTTYgen" and go to "Conversions" → "Import key" from the menu bar.

➤ Private keys created with standard Windows command tools are usually located in the ".ssh" folder directly under the "C:\Users\{username}" folder. "id_rsa" "file".



② Find the key pair you created with another tool and select the private key.

Save the key



Right-click to copy the public key

Any comment can be included

Any Passphrase can be brought

③ Enter a comment and passphrase, and press "Save Private Key" to save the private key.

④ Copy the public key by right-clicking with the mouse. (This step is necessary for the public key registration on the next step.)

➤ If your public key is already registered, this step is not necessary.

Register a public key

Register a public key generated in previous section to the “User Portal”

Copy a public key generated in previous section. Login to the “ABCI User Portal”, open “Register public key” page, select “Direct Input”, paste into the rectangle space, and press [Register].

(If your public key is already registered, this step is not necessary.)

Generated by terminal: Show the generated key by cat command and copy.

```
yourpc$ cat ~/.ssh/id_rsa.pub
ssh-rsa
abcdefghijklmnopqrstuvwxyz1234567890ABCDEFGHI.....
.....EhTBbCel satoshi.kataoka@hanazono.com
yourpc$
```

Login to the “ABCI User Portal” and paste key in “Register public key”

The screenshot shows the ABCI User Portal interface. The page title is "ABCI User Portal" with a login user "Kataoka Satoshi". The main heading is "Register public key". There are four numbered annotations: 1. "Open 'Register public key'" points to the page title. 2. "Select 'Direct input'" points to the "Direct input" radio button under "Registration Method". 3. "Paste the public key here" points to a large text input area. 4. "Press [Register]" points to the "Register" button. A sidebar menu on the left includes links like Home, Change password, Declaration for the Applicability of the Specific Categories, Register public key, Browse / delete public key, Node reservation / cancellation, Usage history for ABCI point, and Cloud Storage Management. A note at the bottom provides instructions for key registration, such as "No line feed character is included" and "In the case of RSA public key, public key must be created with 2048 bits or more."

Generated by “PuTTYgen”: After generate key, copy the public key from the dialog box.

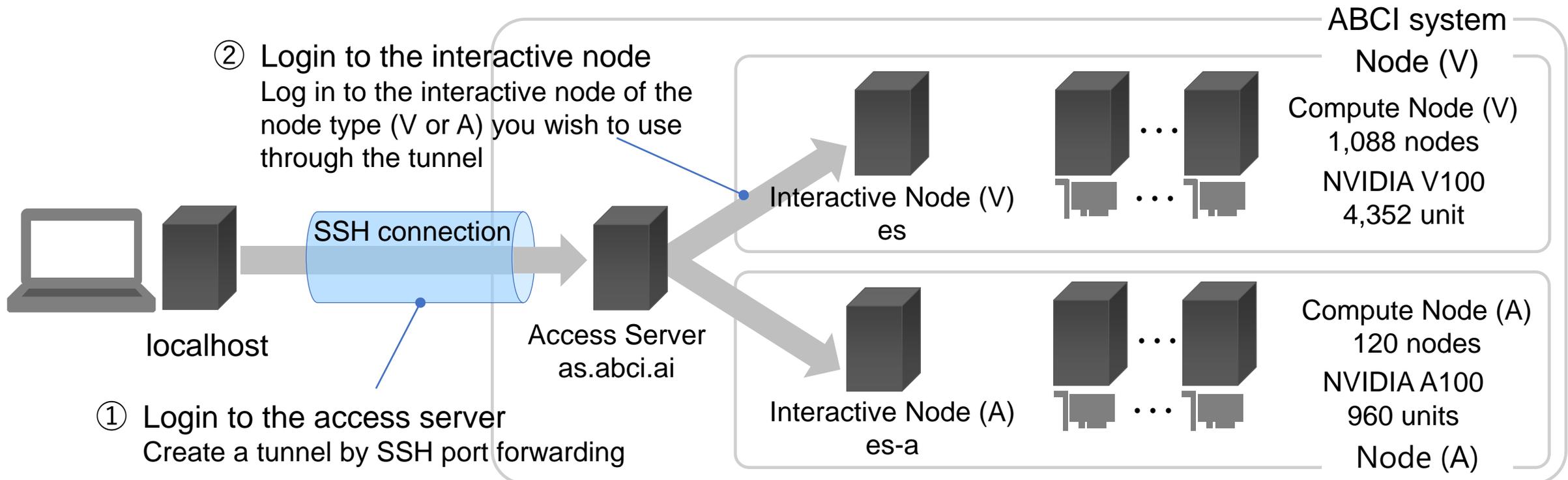
The screenshot shows the PuTTY Key Generator dialog box. The "Key" tab is active, showing a public key for pasting into an OpenSSH authorized_keys file. The key text is highlighted in red. Below the key text, there are fields for "Key fingerprint", "Key comment", "Key passphrase", and "Confirm passphrase".

Drag the public key, right-click in selected area, and choose “Copy”.

Log in to the ABCI system

To connect to an interactive node, which is the front end of ABCI, follow the steps below.

- ① Login to the access server using SSH public key and create a tunnel between the client PC and the interactive node.
- ② Login to the interactive node (es or es-a) through the SSH tunnel using SSH public key authentication.

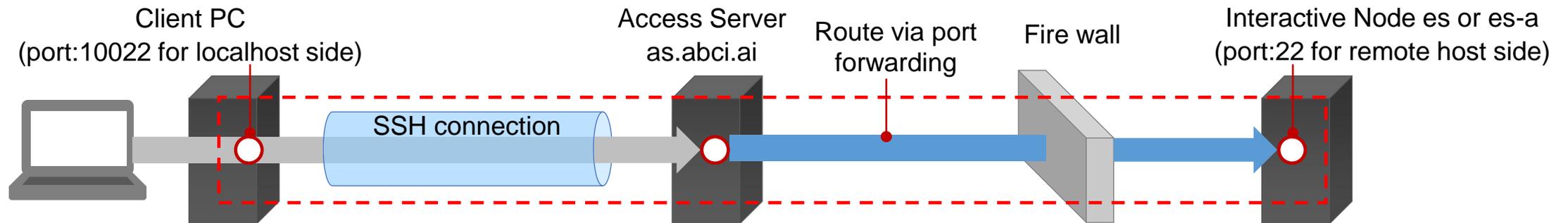


* ABCI has two types of nodes, (V) and (A). Compute Node (V) and Compute Node (A) for Compute nodes, es and es-a for Interactive nodes as well, each of these nodes are dedicated.

Log in to the ABCI system

- Login from Terminal (1/2) -

Login to the access server via SSH and establish a route for port forwarding access from the client PC side to the interactive node. (*The access to the interactive node uses port:22, but the client PC side uses a vacancy number such as port:10022).



Command syntax

```
ssh -L 10022:es:22 -l aaa12345xx as.abci.ai
```

-L {port number to receive on Client PC}:{interactive node name to connect to}:{port number of interactive node} -l {ABCI account name} {access server name}

Create a tunnel between the client PC and the Access Server and port forwarding to the Interactive Node.

Example

```
yourpc$ ssh -L 10022:es:22 -l aaa12345xx as.abci.ai
The authenticity of host 'as.abci.ai (0.0.0.1)' can't be established.
RSA key fingerprint is XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'XX.XX.XX.XX' (RSA) to the list of known hosts.
Enter passphrase for key '/home/username/.ssh/id_rsa':
Welcome to ABCI access server.
Please press any key if you disconnect this session.)
```

This message is shown only at first login.

Type "yes" and [Enter].

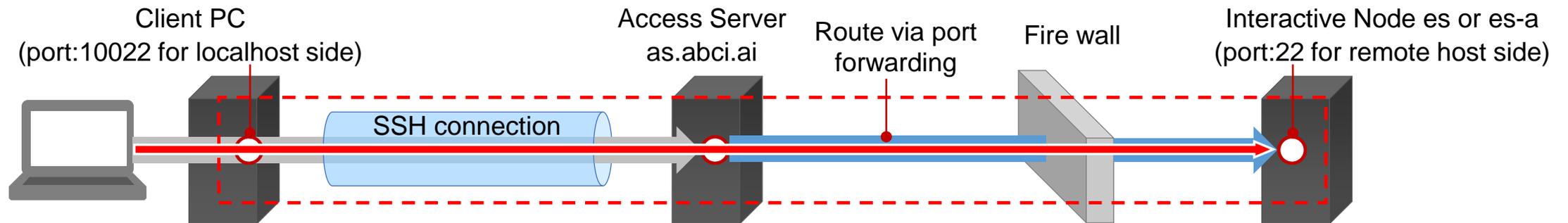
Enter the "passphrase" you set.

After successful login, the message "Welcome to ABCI ..." is appeared.

Log in to the ABCI system

- Login from Terminal (2/2) -

Example: After establishing an SSH connection to the access server (as.abci.ai) and a port forwarding route, open another terminal and login to the interactive node (es) from the configured localhost port:10022.



Command syntax

```
ssh -p 10022 -l aaa12345xx localhost
```

-p {port number to receive on client PC} -l {ABCI account name to login} {host name}

Example

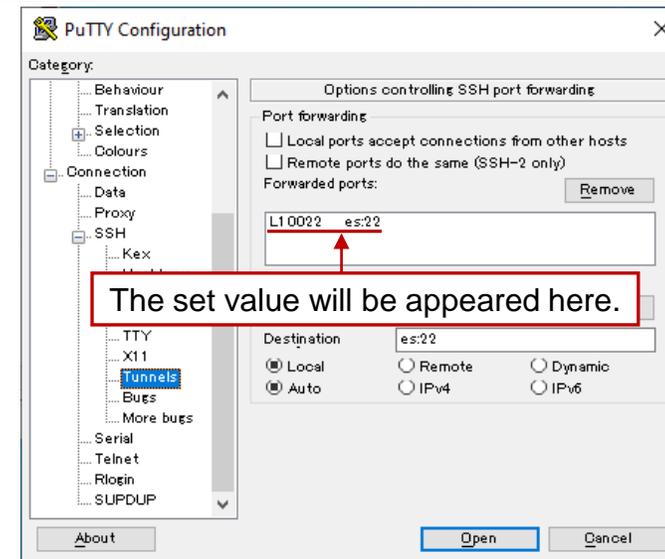
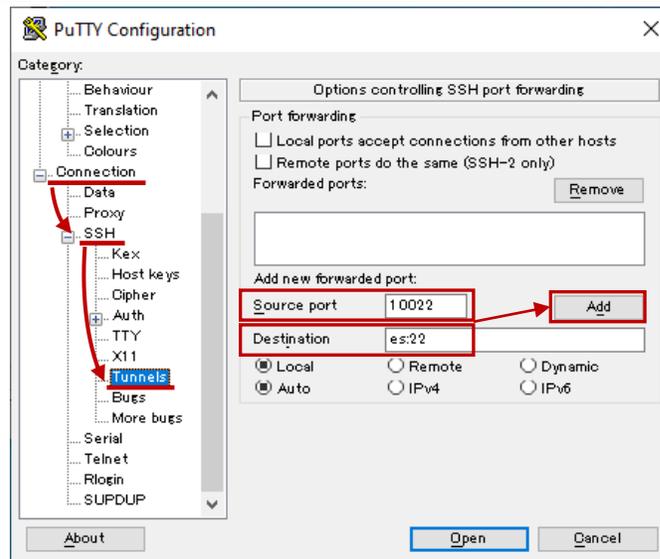
```
yourpc$ ssh -p 10022 -l aaa12345xx localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established. RSA key
XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
Enter passphrase for key '/home/username/.ssh/id_rsa':
[username@es1 ~]$
```

Login to Interactive Node es:22, port forwarded from localhost:10022
 fingerprint is
 This message is shown only at first login.
 Type "yes" and [Enter].
 Enter the "passphrase" you set.
 After successful login, the prompt is appeared.

Log in to the ABCI system

- Using PuTTY (1/6) -

① Open PuTTY and set SSH tunnel parameters.

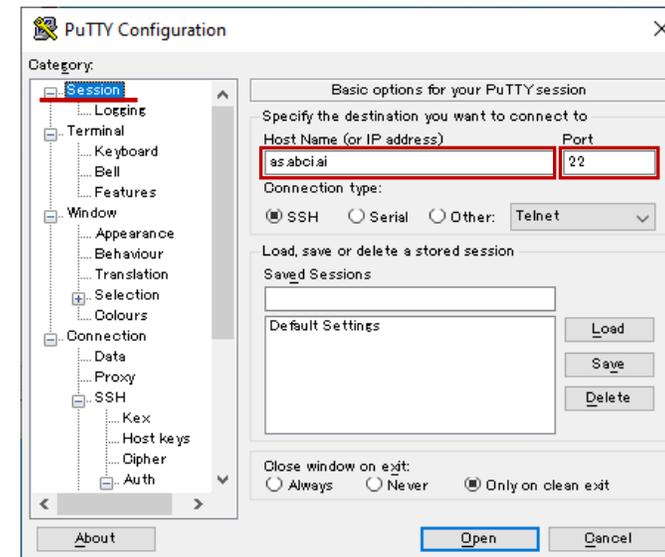
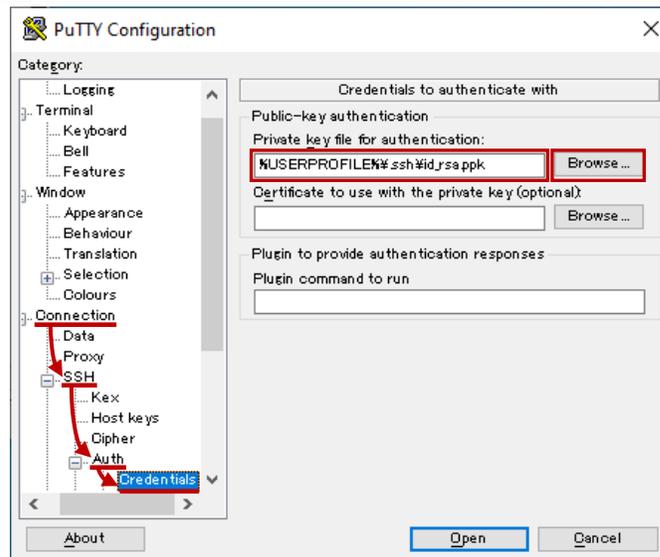


- ① In the Category menu on the left side of the dialog box, select “Connection” => “SSH” => “Tunnels”, then fill in the following values in the “SSH port forwarding” field on the right.
- ✓ Source port: 10022 (Specify a vacancy port number in your system)
 - ✓ Destination: es:22 or es-a:22
 - ✓ Choose “ Local”
- After entering the setting values, press the [Add] button to reflect the setting values.

Log in to the ABCI system

- Using PuTTY (2/6) -

② Enter the SSH authentication information.



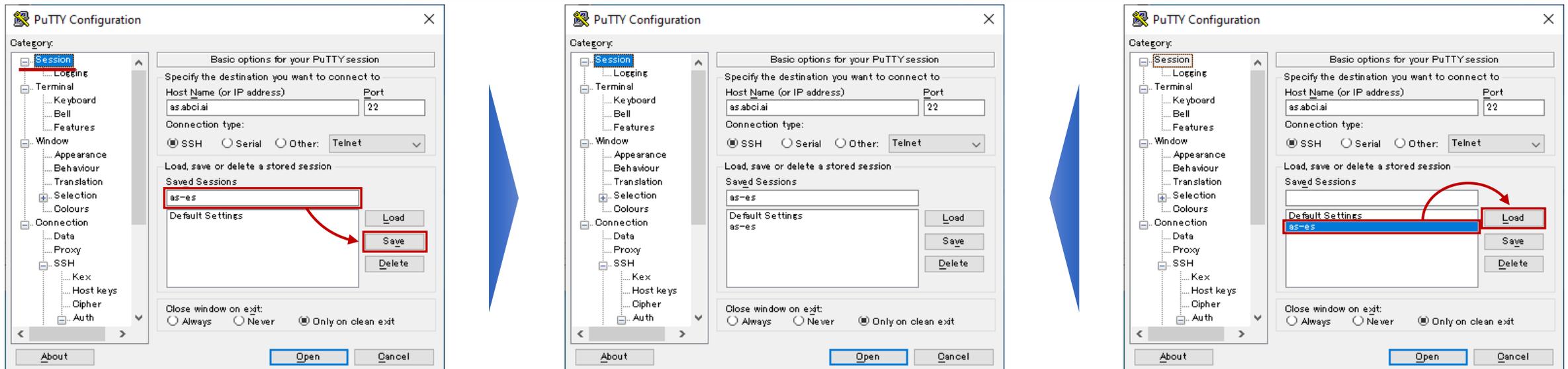
- ② - 1. In the Category menu on the left side of the dialog box, select “Connection” => “SSH” => “Auth” => “Credentials”, then specify the path to the private key in the “Public-key authentication” field.
- ✓ Private key file for authentication: Enter the path to the private key.
 - ✓ You can also select a file by pressing the [Browse] button.

- ② - 2. Page “Session” in the Category menu on the left side and enter login parameters.
- ✓ Host Name (or IP address): as.abci.ai
 - ✓ Port: 22

Log in to the ABCI system

- Using PuTTY (3/6) -

③ Save and load the set parameters.

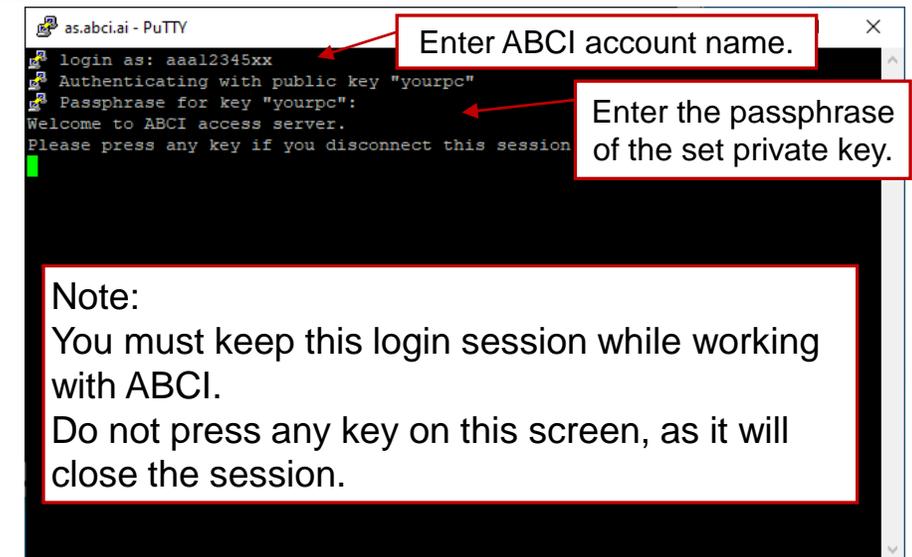
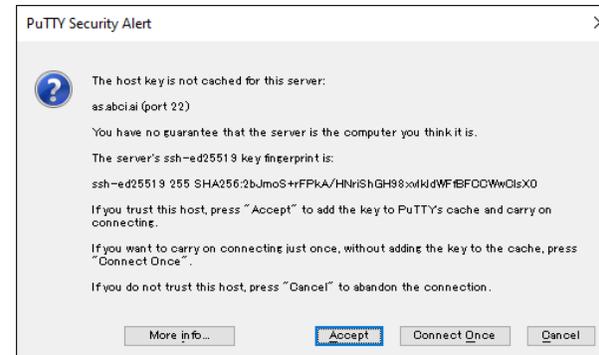
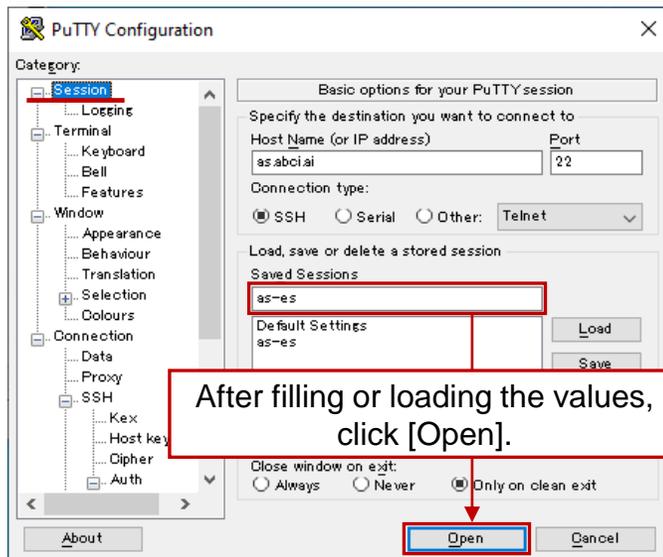


- ③ - 1. Name and save the settings entered so far.
Enter "as-es" in the "Saved Sessions" field and press the [Save] button to place it on the saved list.
2. When you want to reuse the saved settings, select them from the save list and press the [Load] button to recall them.

Log in to the ABCI system

- Using PuTTY (4/6) -

④ Log in to the access server (as.abci.ai) and create an SSH tunnel.

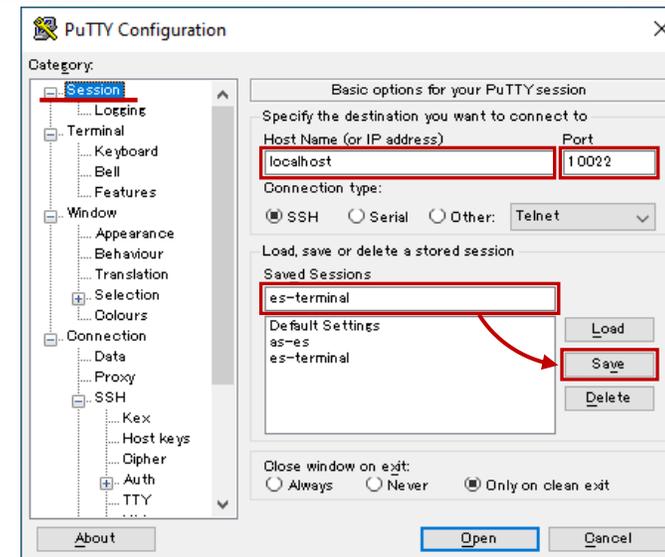
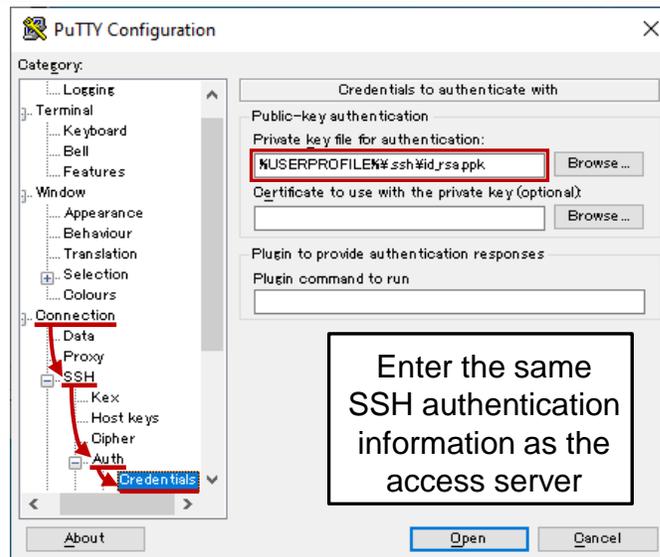


- ④ - 1. After all values are entered or loaded, press the [Open] button.
2. When logging in for the first time, you will see the message in the center above and press the [Accept] button.
3. The access server login screen will be displayed, enter the following...
 - ✓ "ABCI Account Name"
 - ✓ "Passphrase" of the private key
 If the login is successful, "Welcome to ABCI Access Server" will be displayed.

Log in to the ABCI system

- Using PuTTY (5/6) -

⑤ Launch PuTTY in another window and configure the connection settings



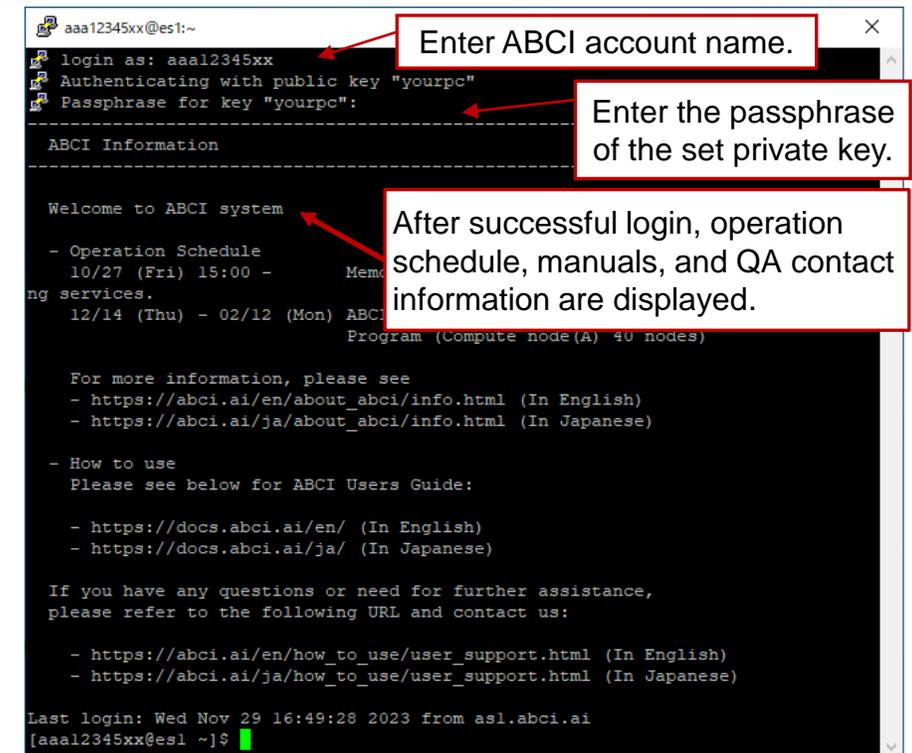
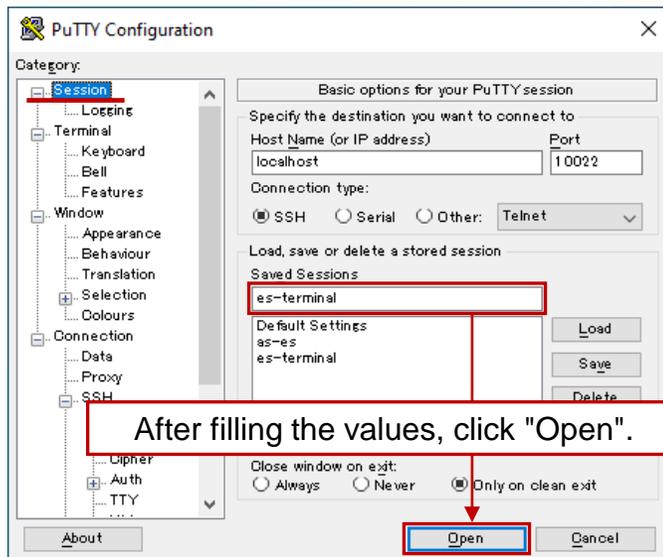
- ⑤ - 1. In the Configuration dialog box of PuTTY launched in another window, select “Connection” => “SSH” => “Auth” => “Credentials” from the Category menu on the left, then specify the path to the private key in the “Public-key authentication” field, in the same way as for the access server.

- ⑤ - 2. Select “Session” from the Category menu on the left, enter the login information for the Interactive Node.
- ✓ Host Name (or IP address): localhost
 - ✓ Port: 10022
- Specify the port number set in the SSH Tunnel Information. Enter the same SSH authentication information as the Access server.
- After entering the configuration parameters, save them again as a name, e.g., “es-terminal”.

Log in to the ABCI system

- Using PuTTY (6/6) -

⑥ Log in to the Interactive Node (es or es-a).



- ⑥ - 1. After all values are entered or loaded, press the [Open] button.
2. When logging in for the first time, you will see the message in the center above and press the [Accept] button.
3. The Interactive Node login screen will be displayed, enter the following...
- ✓ "ABCI Account Name"
 - ✓ "Passphrase" of the private key
- If the login is successful, "Welcome to ABCI System" will be displayed.

Reference Links Summary

- ABCI Official Website (<https://abci.ai/>)

- ABCI 2.0 User Guide (<https://docs.abci.ai/en/>)

This guide explains the technical details of ABCI 2.0 and how to use it.
This content mainly introduces the "Connecting to Interactive Node" section in the "Getting Started ABCI" chapter of the User Guide.

- ABCI Portal Guide (<https://docs.abci.ai/portal/en/>)

A portal site for managing ABCI 2.0 users and other necessary information.

- Windows Subsystem for Linux (WSL)

Reference information on the environment settings required to use ABCI2.0 from Windows terminals.
Please refer to the latest information as it is updated from time to time on external sites.

- <https://learn.microsoft.com/en-us/windows/wsl/install#manual-installation-steps>
- <https://qiita.com/fumikomatsu/items/01e5cfa09347176f4d1a> (Japanese)
- <https://chigusa-web.com/blog/wsl2-win11/> (Japanese)

- About SSH client software PuTTY

- WinSCP (included PuTTYgen, <https://winscp.net>)
- PuTTY (<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>)

