

---

# **Supercomputer Fugaku Startup Guide Version 1.06**

**RIKEN Center for Computational Science**

**Jun 22, 2022**

## INDEX:

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	The purpose of this document. . . . .	1
1.2	Notation used in this document . . . . .	1
1.3	About trademarks . . . . .	1
1.4	Change log . . . . .	1
<b>2</b>	<b>System Use</b>	<b>3</b>
2.1	Overview . . . . .	3
2.2	Client Certification Installation . . . . .	5
2.2.1	Installing the certificate to Firefox (Windows) . . . . .	5
2.2.2	Installing the certificate on Firefox (Mac) . . . . .	10
2.2.3	Installing the certificate to Chrome (Windows) . . . . .	14
2.2.4	Installing the certificate to Chrome (Mac) . . . . .	22
2.3	Accessing steps to the user portal . . . . .	26
2.4	Login . . . . .	27
2.4.1	Private key/Public key creation . . . . .	28
2.4.2	Public key registration . . . . .	31
2.4.3	Accessing direction . . . . .	33
2.4.4	File transfer method . . . . .	37
2.4.5	Login shell . . . . .	40
2.4.6	E-mail distribution of Fugaku operation information . . . . .	40

## INTRODUCTION

### 1.1 The purpose of this document.

This document describes about the required settings to use Supercomputer Fugaku after finishing the account registration.

Please proceed the initial settings such as client following this document. After the initial settings, access to the user portal ( <https://www.fugaku.r-ccs.riken.jp/en> ) and refer to the Users Guide.

### 1.2 Notation used in this document

- In command execution, the user terminal and login node to be operated are represented by a prompt.

Prompt	Control target
[terminal]	Means to execute the command at the user device
[_LNlogin]	Means to execute the command at the login node (Common)

- Home directory indicates with ~ (tilde).

### 1.3 About trademarks

Company names and product names in the text may be trademarks or registered trademarks of the respective companies. Other trademarks and registered trademarks are generally trademarks or registered trademarks of their respective companies. Please note that trademark names (TM, (R)) are not always added to system names, product names, etc., described in this document.

### 1.4 Change log

This indicates the update history of this document.

#### Version 1.06 June 22, 2022

- Added flow diagram to “2.1 Overview”.

#### Version 1.05 June 6, 2022

- Indicates that we plan to ban the use of RSA in “2.4.1 Creating a Private/Public Key Pair”.

#### Version 1.04 May 23, 2022

- Added a note about permissions to “2.4 login”.

#### Version 1.03 April 6, 2022

- Added a note about using [Chrome@Mac](#) in “2.3 Accessing steps to the user portal”.

**Version 1.02 April 3, 2022**

- Added “2.4.6. E-mail distribution of Fugaku operation information”.

**Version 1.01 April 15, 2021**

- Updated the description of “Client certificate passphrase” in “2.2. Client Certification Installation”

**Version 1.00 March 4, 2021**

- Changed the host name of login node.
- Updated step 1 of “2.2.3. Installing the certificate to Chrome (Windows)”
- Updated of “2.4.2. Public key registration”

**Version 0.2 November 27, 2020**

- Added “Change log”.
- Changed the note about browser in “2.3. Accessing steps to the user portal”.
- Updated step 5 of “2.4.2. Public key registration”

© 2022 RIKEN Center for Computational Science

Unauthorized reproduction or duplication of the contents described in this manual is prohibited.

**SYSTEM USE**

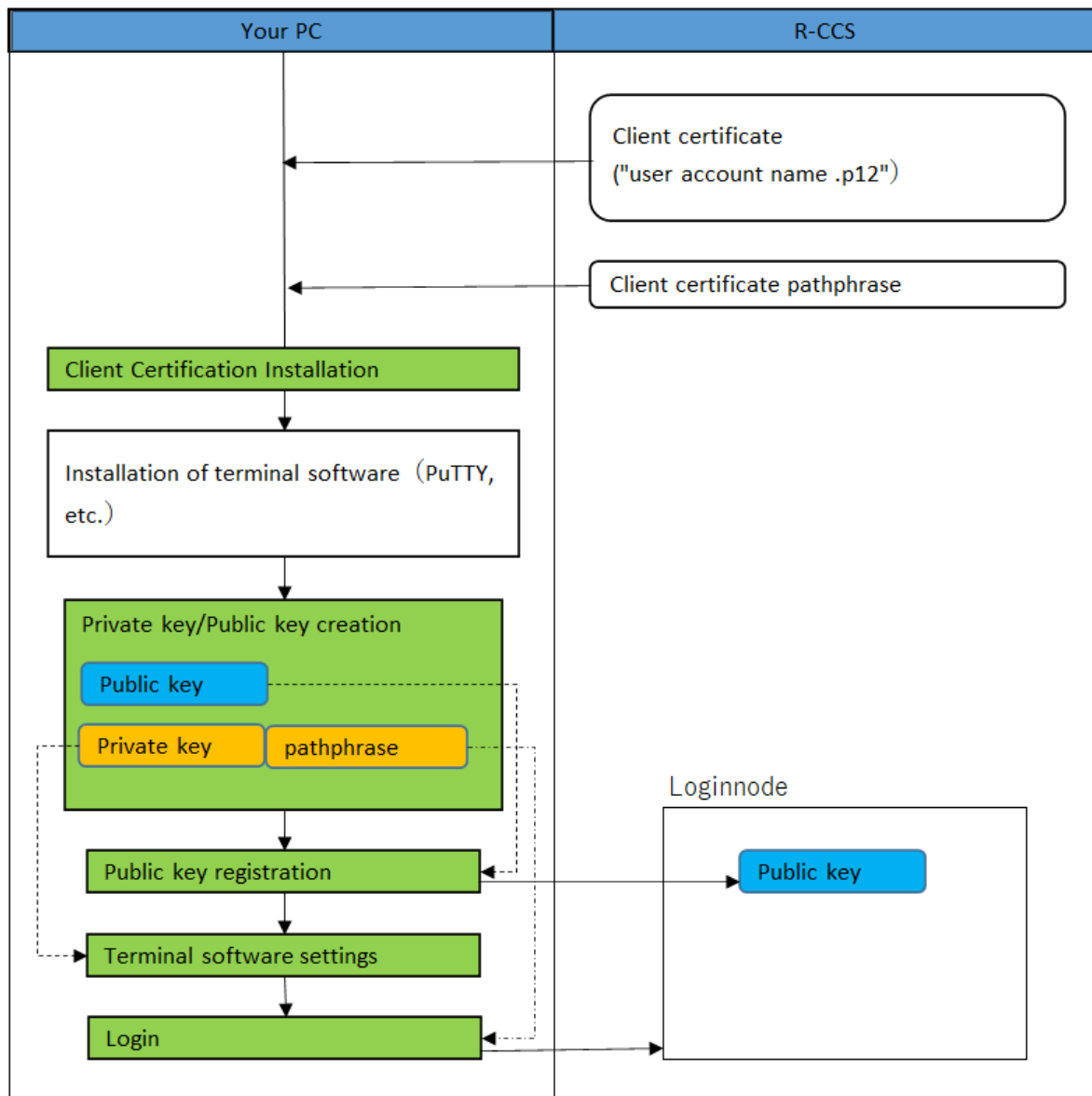
This section describes the basic items such as logging into the system, for use of Supercomputer Fugaku.

## **2.1 Overview**

To use the Supercomputer Fugaku, you need to use portal site and login node.

Here describes the installation procedure of client certificate which is required for using the portal site, and the creation and registration procedure of SSH public key which is required to connect the login node.

The flow of setting is as follows:.



Item	Reference to
Client Certification Installation	<i>Client Certification Installation</i>
Private key/Public key creation	<i>Private key/Public key creation</i>
Public key registration	<i>Public key registration</i>
Terminal software settings	<i>Login node (PuTTY)</i>
Login	<i>Login node (PuTTY)</i>

## 2.2 Client Certification Installation

Client certificate is used when accessing to the user portal. Please install to the browser which accesses to the user portal.

This indicates how to install the required client certificate to access to the user portal of Supercomputer Fugaku. This work is not required if installed the client certificate by referring to the Startup Guide.

Please prepare the followings before installing the client certificate.

- Client certificate : "user account name .p12" file
- Client certificate pathphrase

**Client certificate** Once the account issue is completed, the client certificate is sent via e-mail to the e-mail address you entered when applying. Please save the attached "local account name.p12" file to the device (e.g. PC) which installs the client certificate. To "local account name.p12" file, the client private key, the client certificate (a public key) and the route certificate of the client certificate issuing authority.

**Client certificate pathphrase** The passphrase is sent in written form or PDF file separately from the client certificate. It will be required when installing the client certificate. Please store at the safe place.

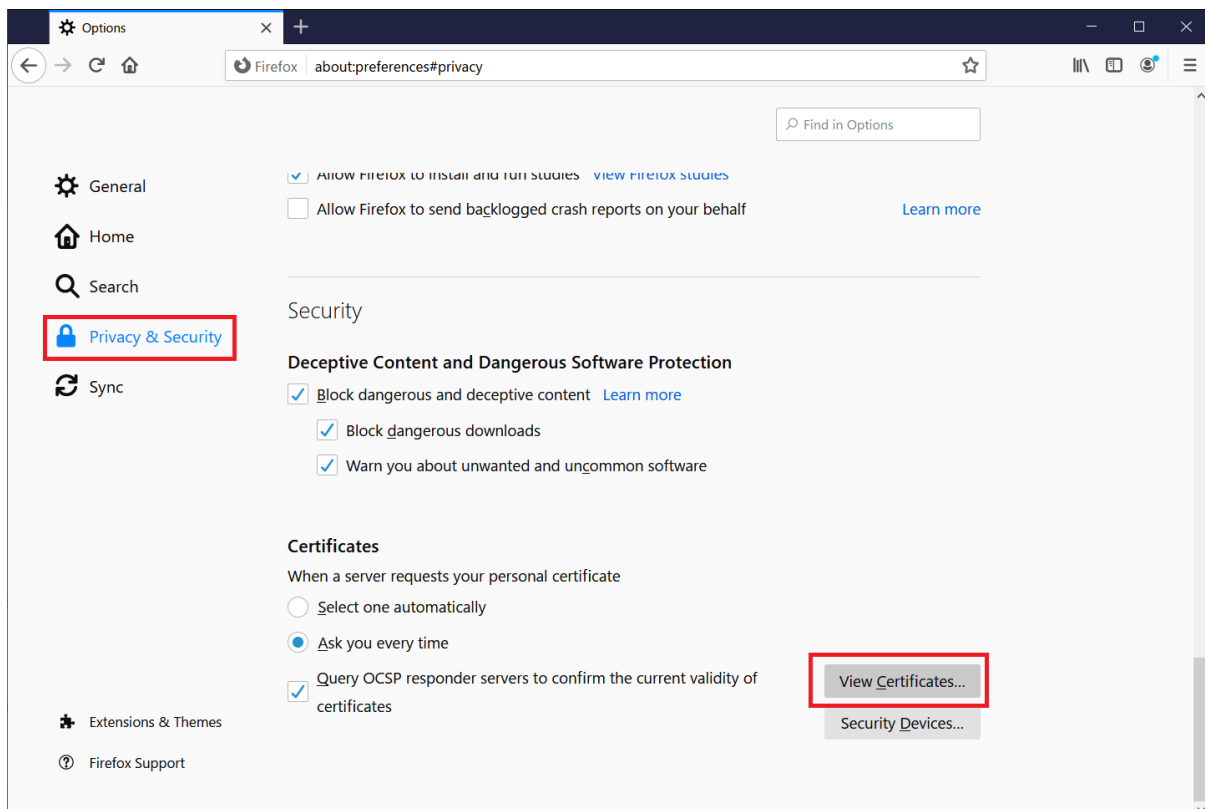
This section describes the procedure for registering a client certificate on your PC.

**Note:** If you use a different browser than the specified browser, confirm the certificate management method of the browser yourself, and install the client certificate in the browser to be used.

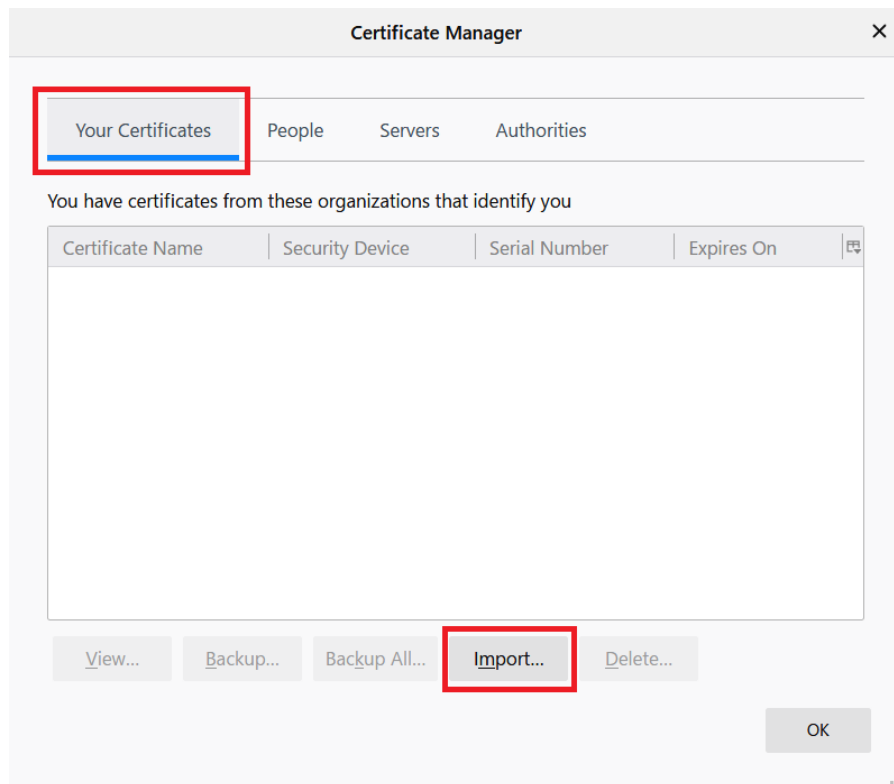
### 2.2.1 Installing the certificate to Firefox (Windows)

This indicates how to install Firefox on Microsoft Windows. The difference may be seen depending on the version of Firefox. If the screen is different, please try with confirming the Firefox information.

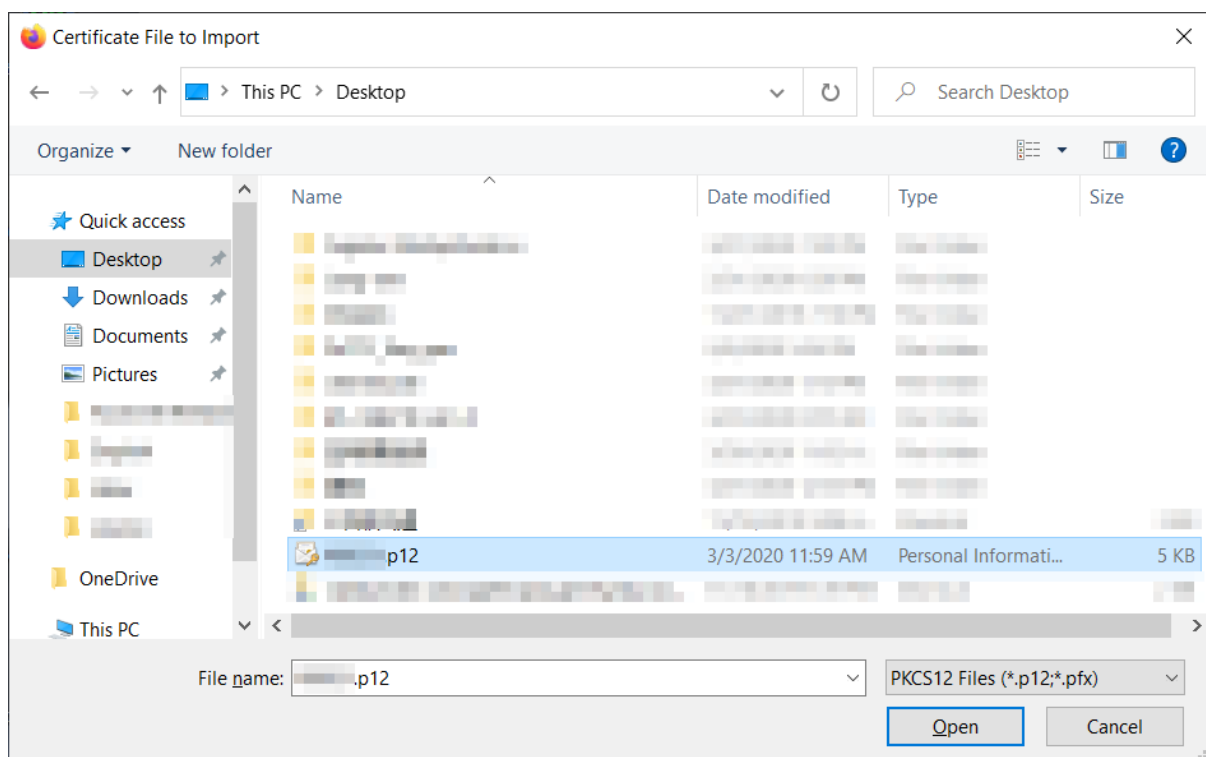
1. Start Firefox and open [Option]. Click on [Privacy and Security]'s [Display certificate].



2. Once the certificate manager is started, select *[Your Certificates]* and click on *[Import...]*.

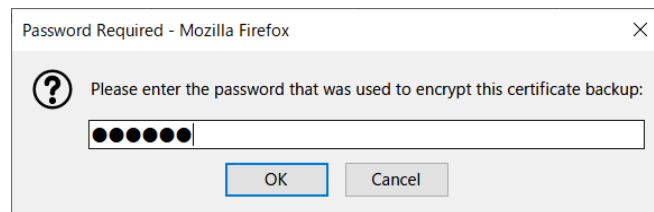


3. Client certificate: Select “local account name.p12” file and click on *[Open]*.



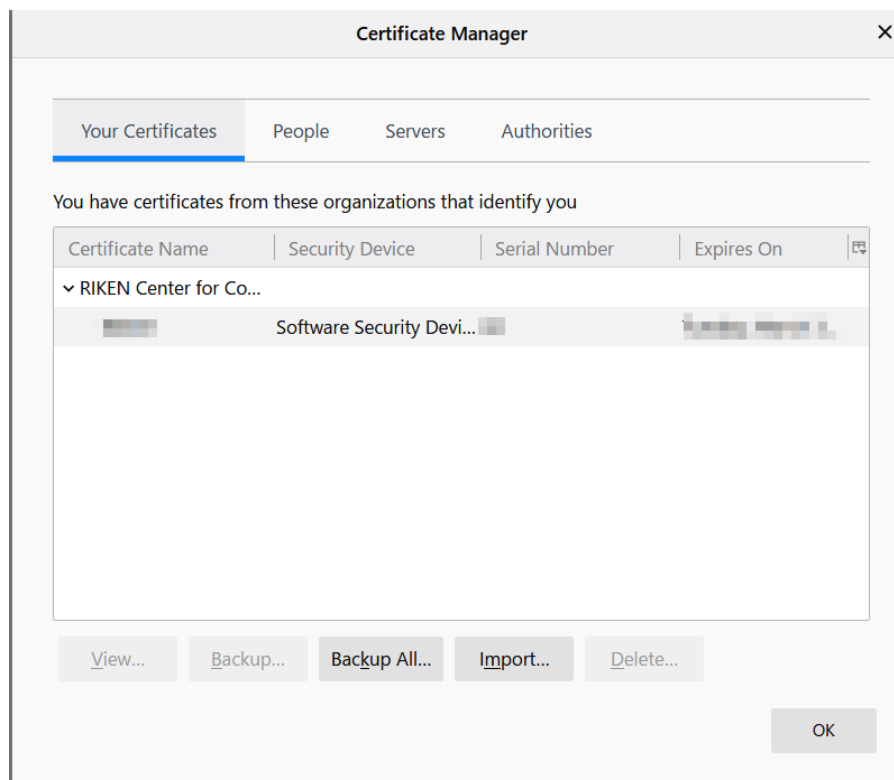


4. Input the client passphrase to *Password* and click on [OK].

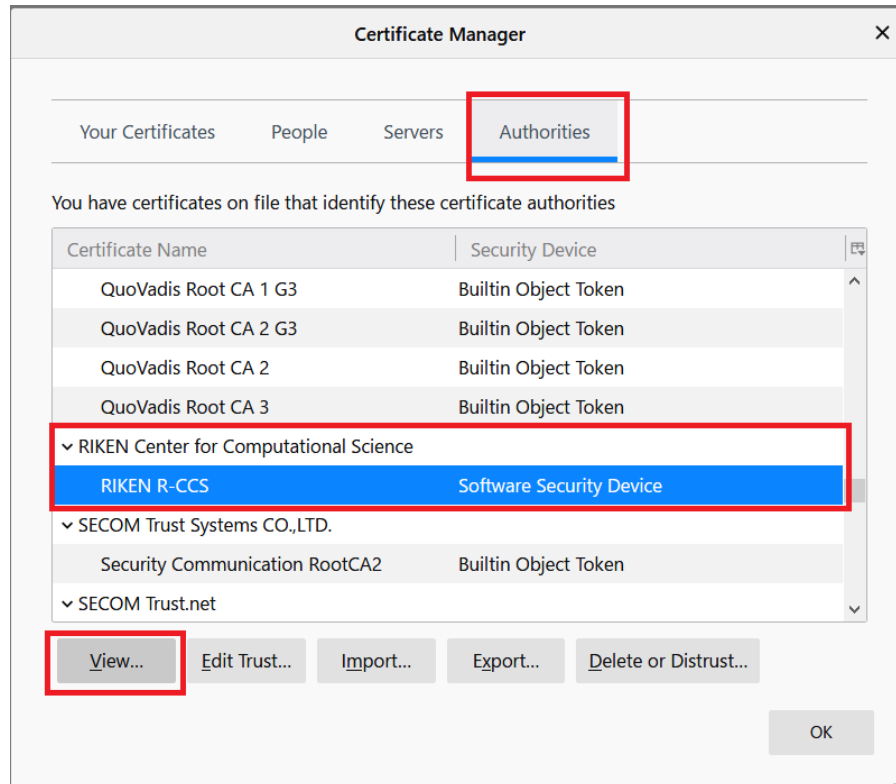


**Attention:** If the client certificate passphrase is wrong it shows an error and cannot go forward.

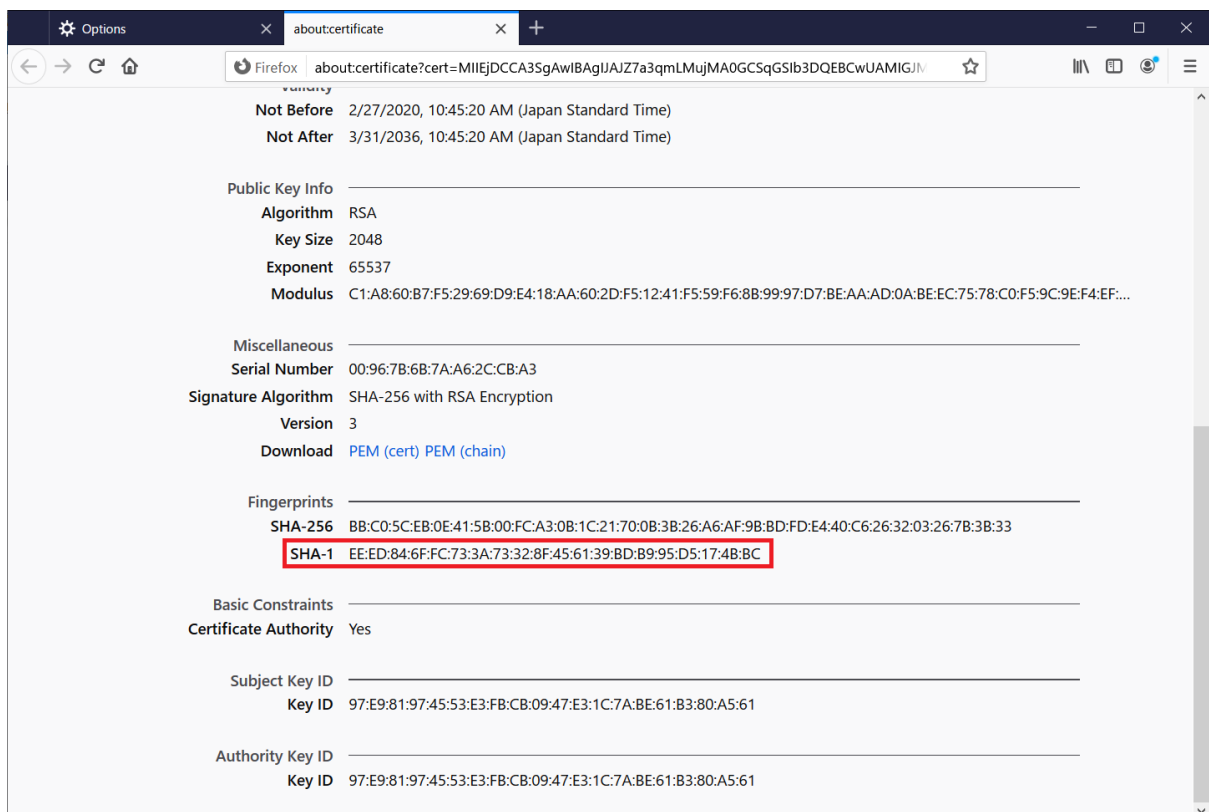
5. Confirm if the client certificate is registered.



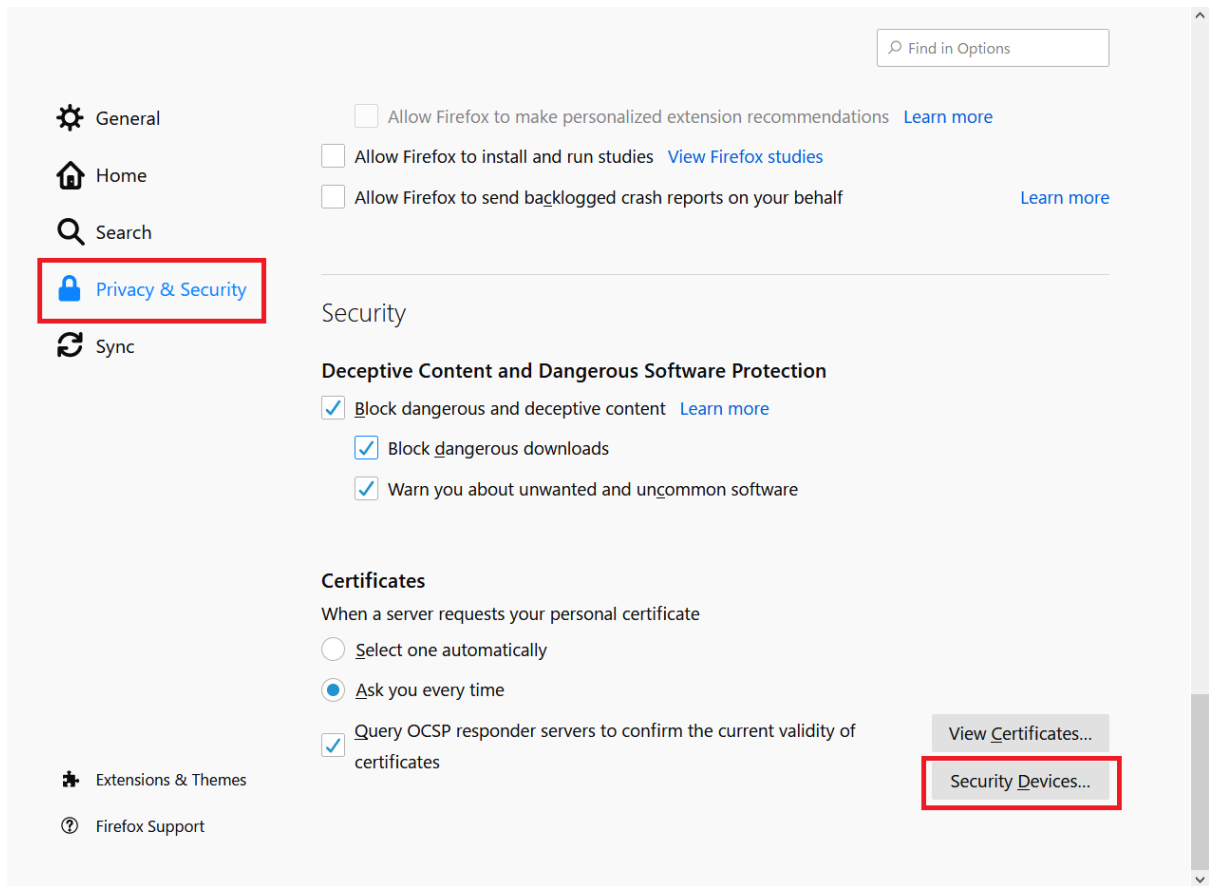
6. Select [Authorities] and from the list, select “RIKEN R-CCS” and click on *View...*



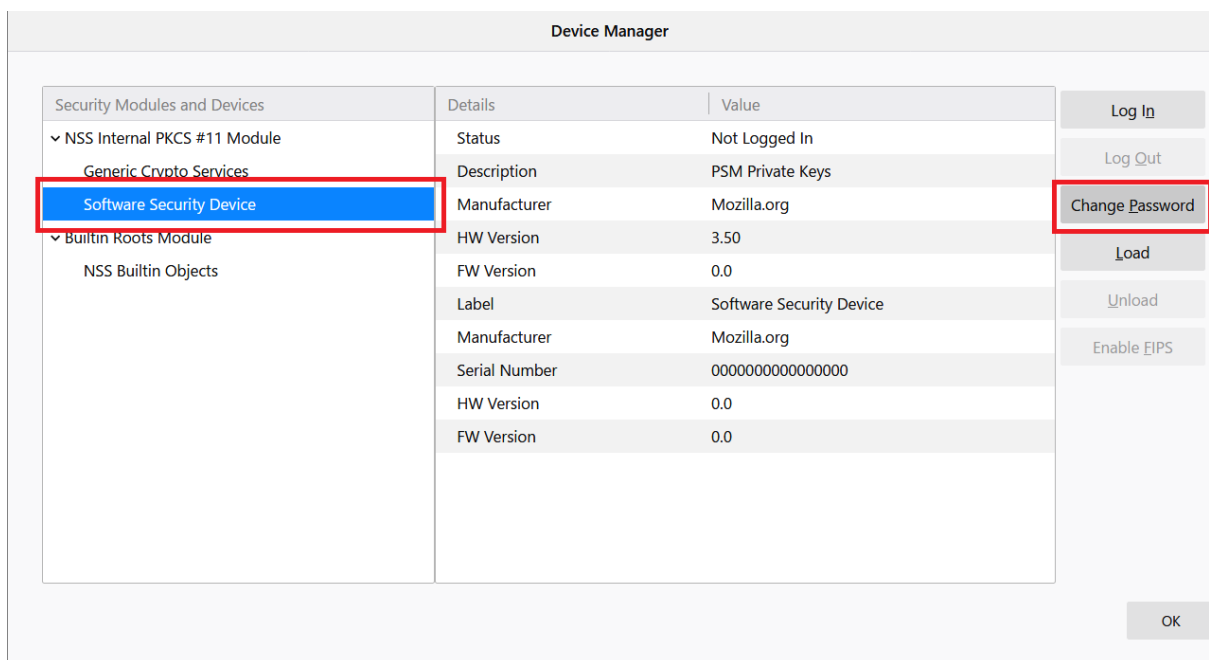
7. Please confirm if the certificate's Fingerprints is (SHA-1): EEED846F FC733A73 328F4561 39BDB995 D5174BBC.



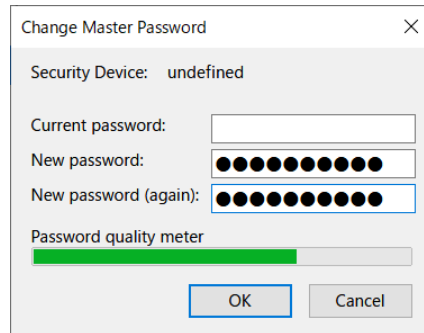
8. Next, set the password to be entered when using the client certificate. Click on *Security Devices...*



9. Once device manager is started, select *Software Security Device* and click on *Change password*.



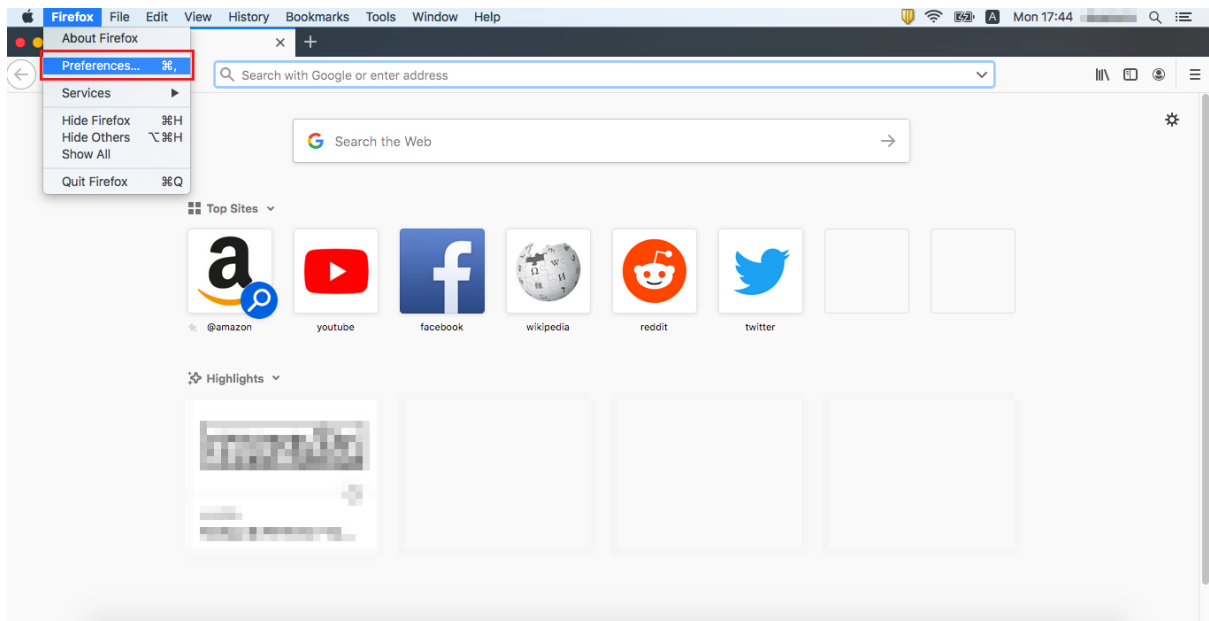
10. Set any password required when using the client certificate, click on *OK*.



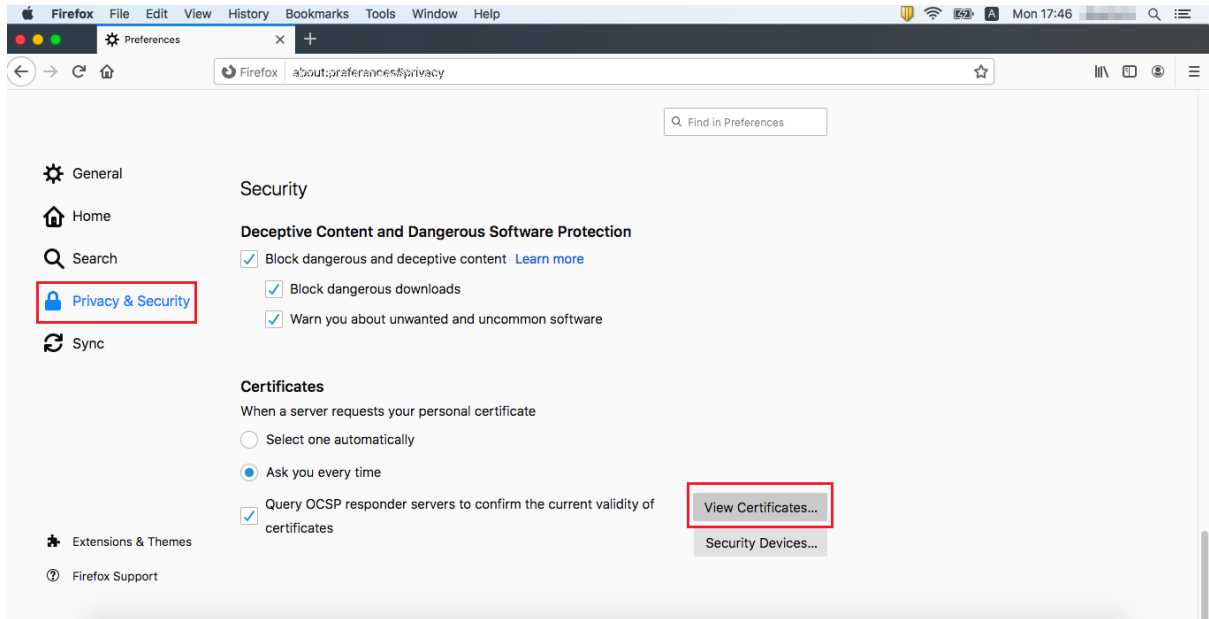
11. After registering the password, close Device Manager. This is the end of setting the password when using the client certificate. The password set here is used when using the client certificate.

## 2.2.2 Installing the certificate on Firefox (Mac)

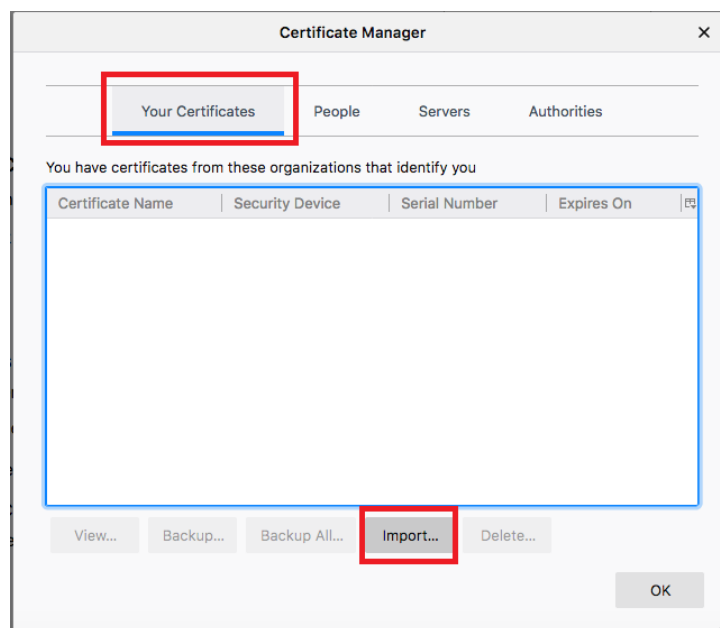
1. Start Firefox, then click [*Preferences...*] from menu.



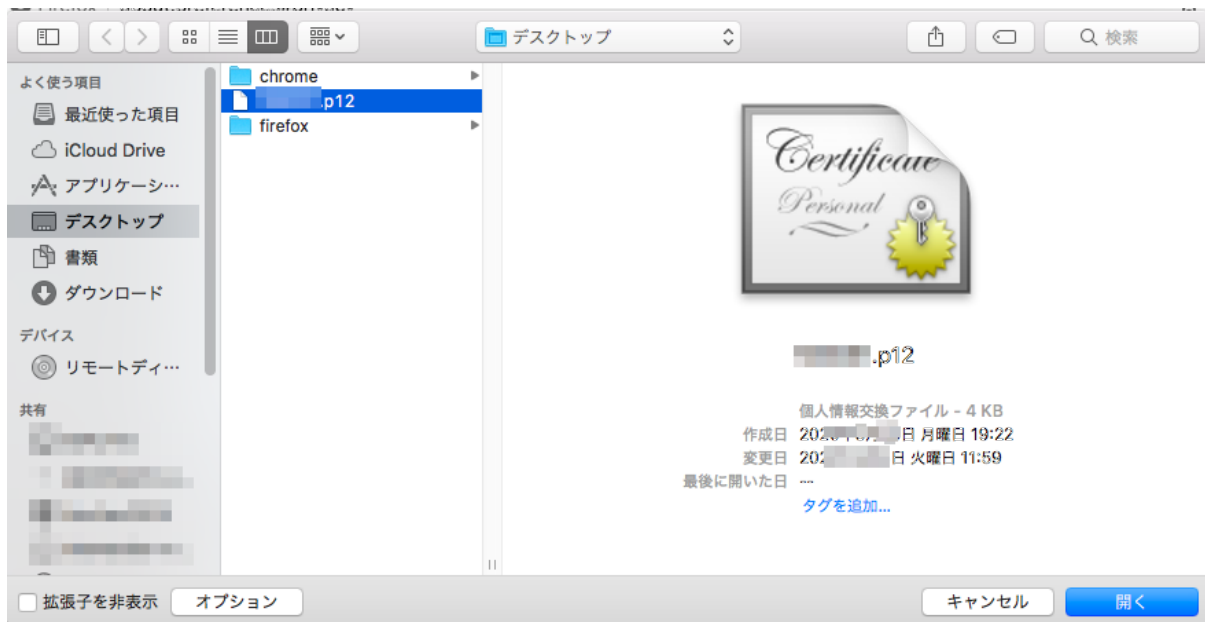
2. Click [*View certificates...*] in *Privacy and security* tab.



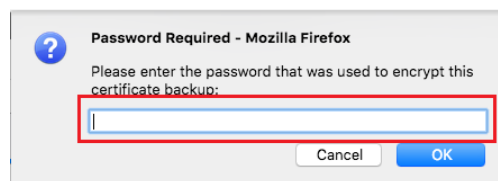
3. Once certificate manager started, select *[Your certificate]* then click *[Import...]*.



4. Select the “local account name.p12” file saved on your computer, click *[Open]*.

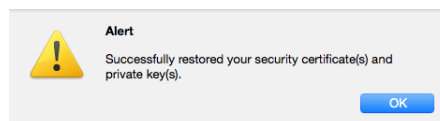


5. Input the passphrase of the obtained client certificate to *Password area*, click [OK].

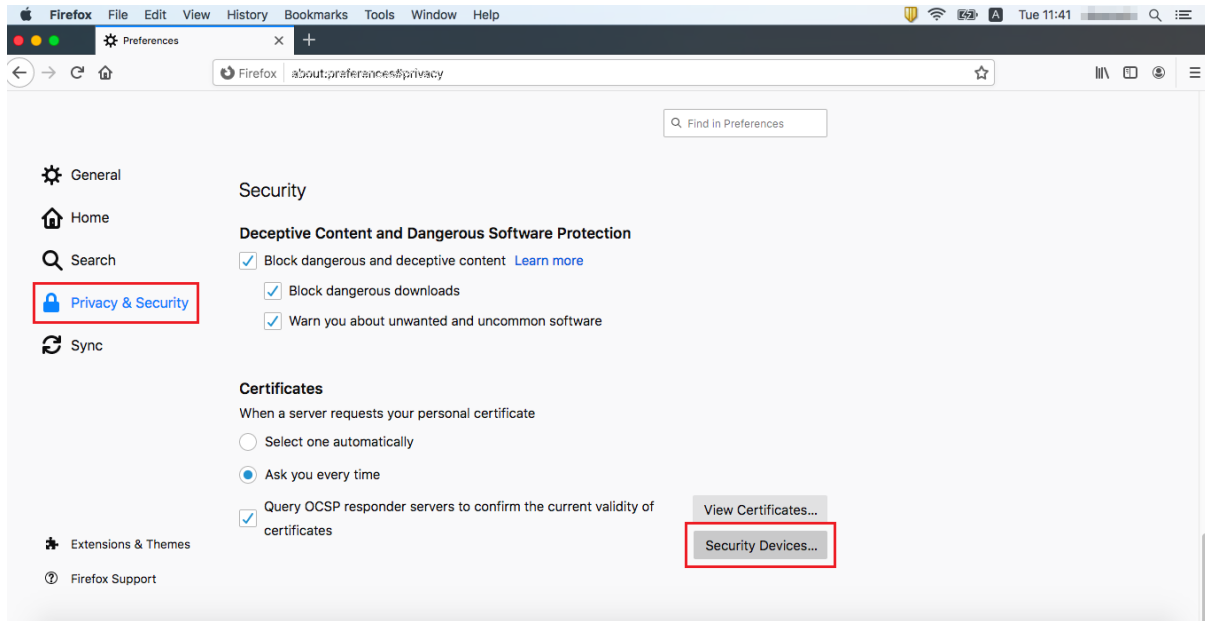


**Attention:** If the client certificate passphrase is incorrect, an error is displayed and you cannot proceed to the next screen.

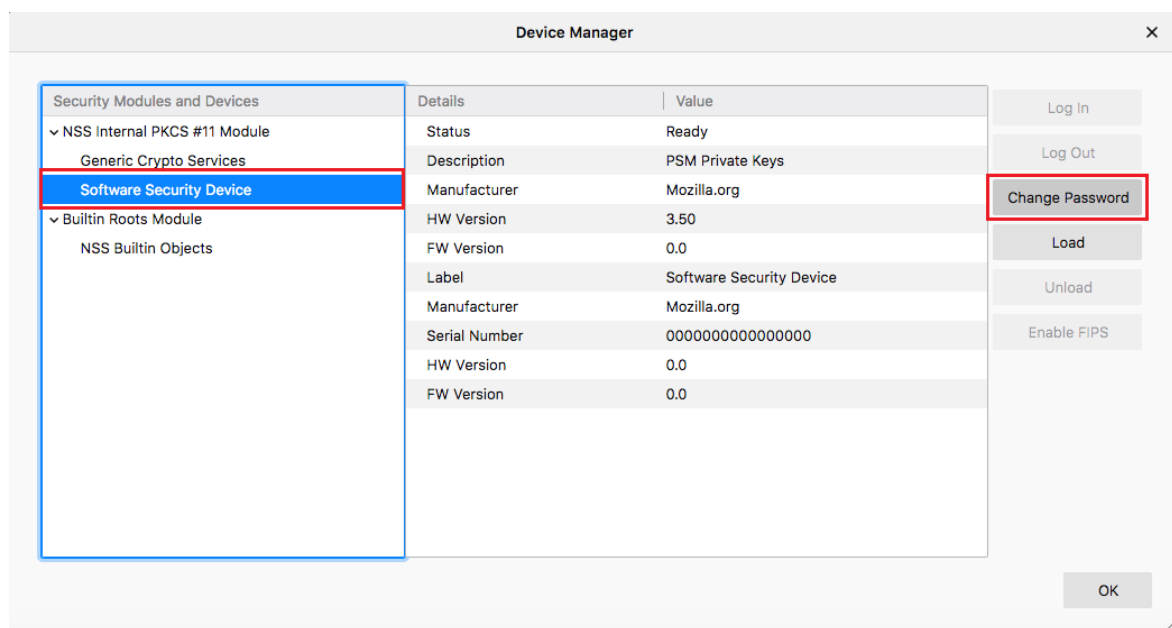
6. Confirm that the client certificate has been registered, click [OK] and close the certificate manager. This completes the client certificate installation process.



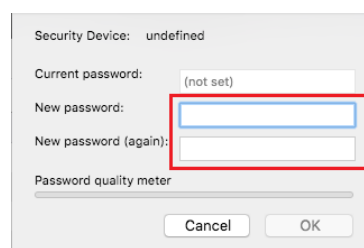
7. Next, set the password to be entered when using the client certificate. Click *Security device...*



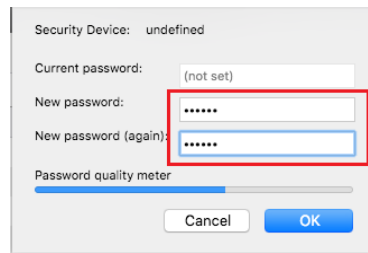
8. Once device manager starts, select *Software Security Device* then click *Change password...*



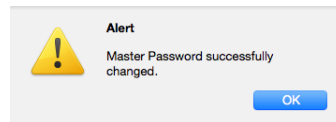
9. Set an arbitrary password required when using a client certificate, click *OK*.



10. Click *OK*.



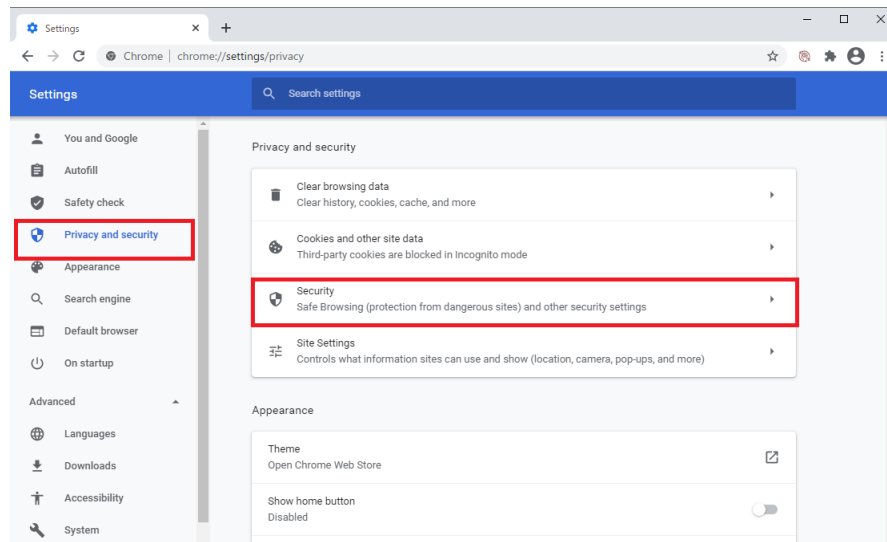
11. Click *OK* and close device manager. This completes the password setting procedure when using a client certificate.



### 2.2.3 Installing the certificate to Chrome (Windows)

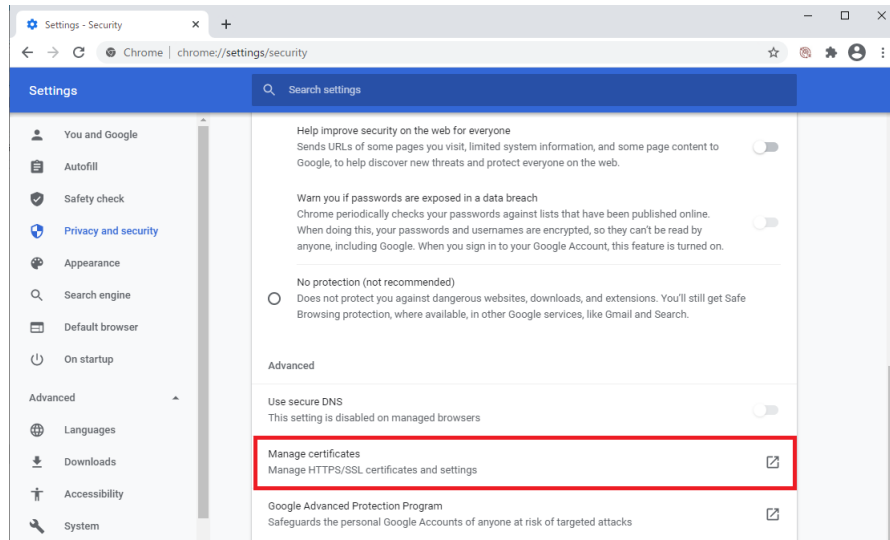
This indicates how to install Chrome on Microsoft Windows. The difference may be seen depending on the version of Chrome. If the screen is different, please try with confirming the Chrome information.

1. Start Chrome and open *[Settings]*. Click on *[Privacy and security]*'s *[Security]*.

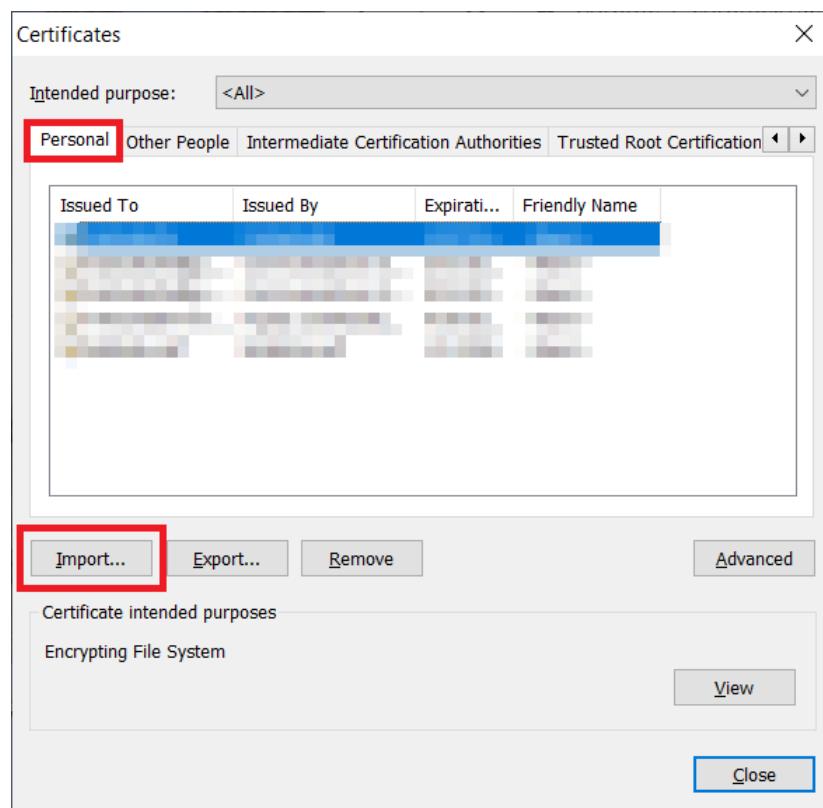


2. Click on *[Manage certificates]*.

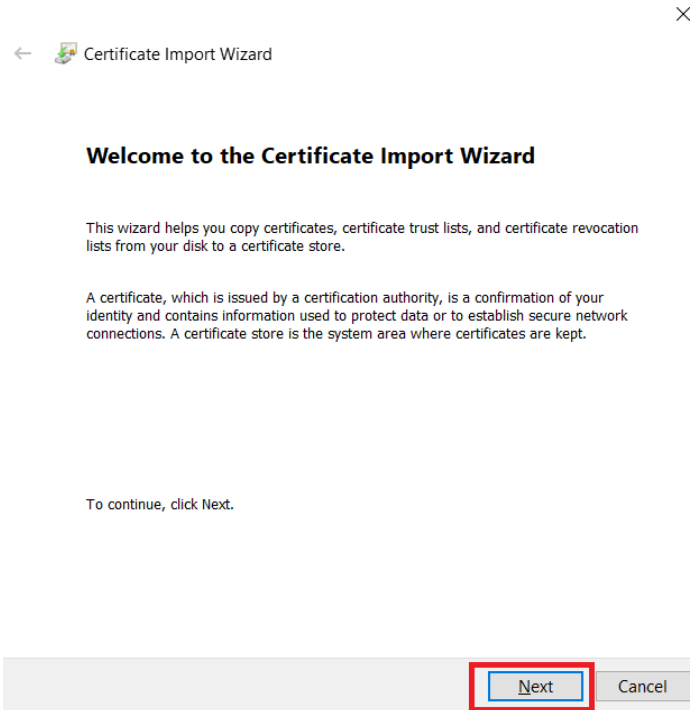




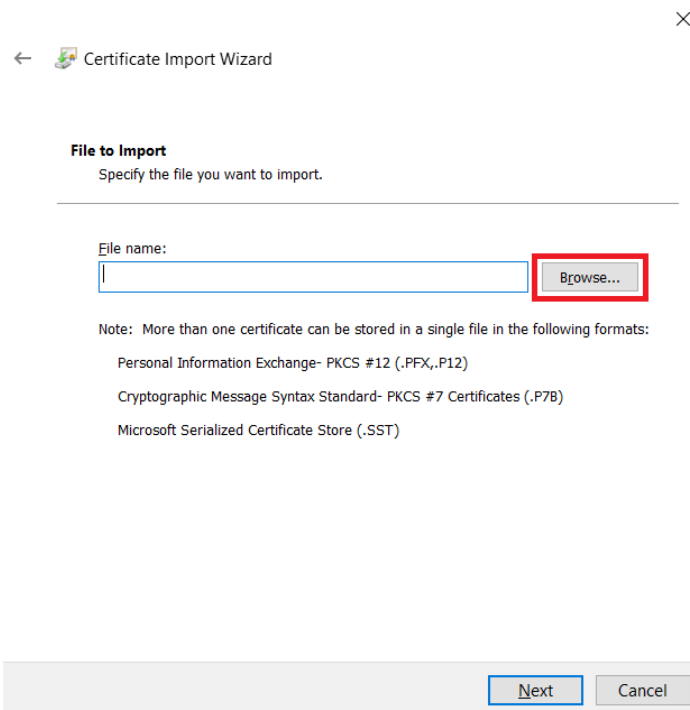
3. Once certification manager is started, select *[Personal]* and click on *[Import...]*.



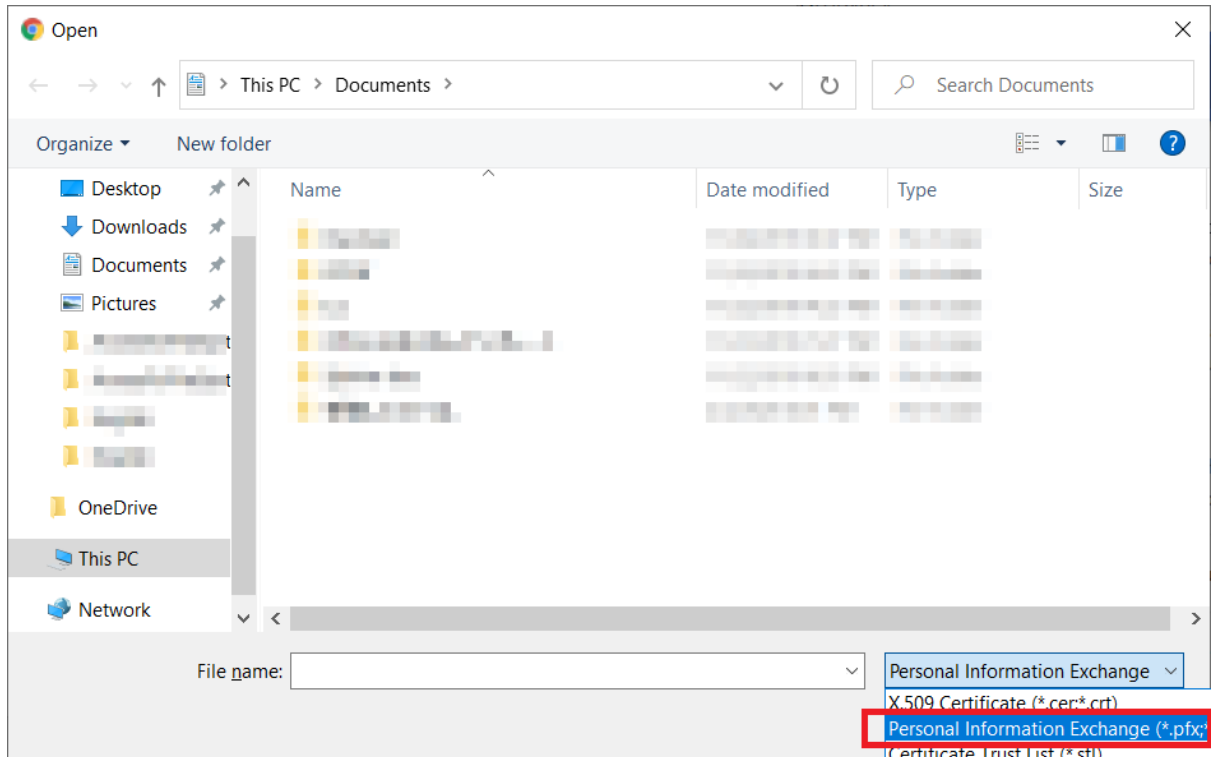
4. Once certificate import wizard is opened, click on *[Next]*.



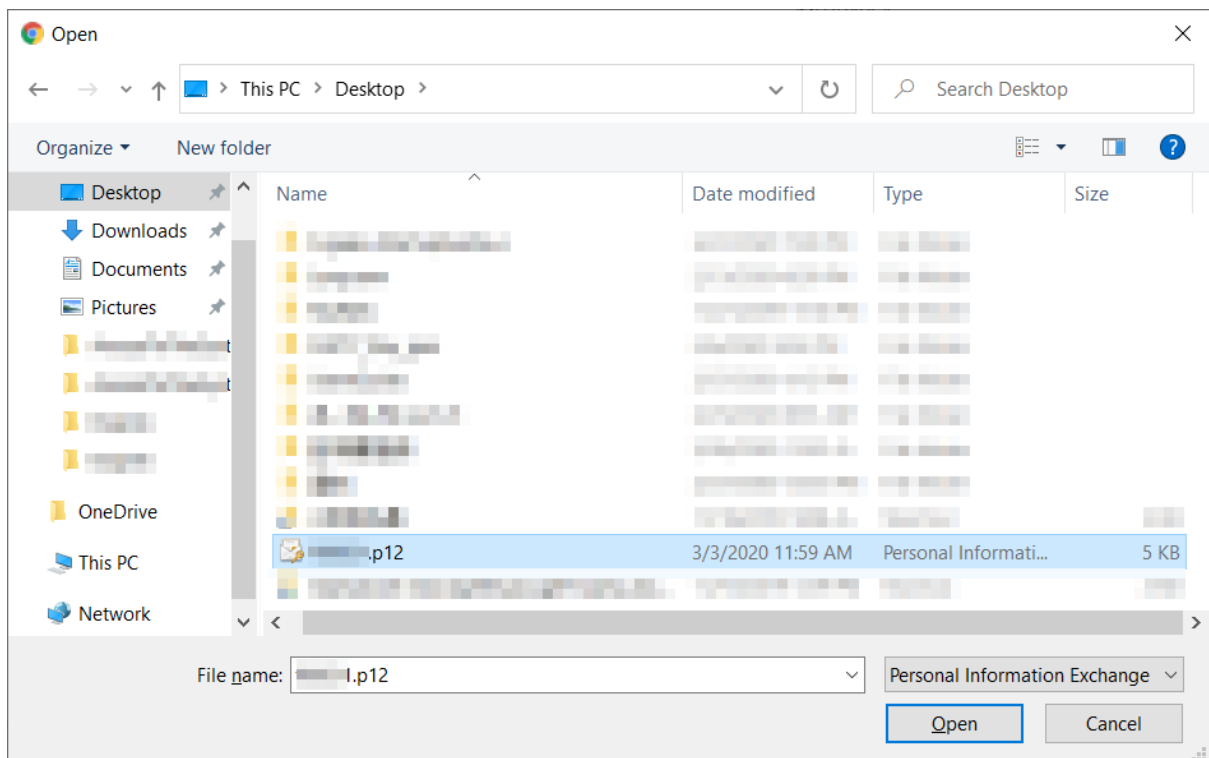
5. Click on *[Browse...]*.



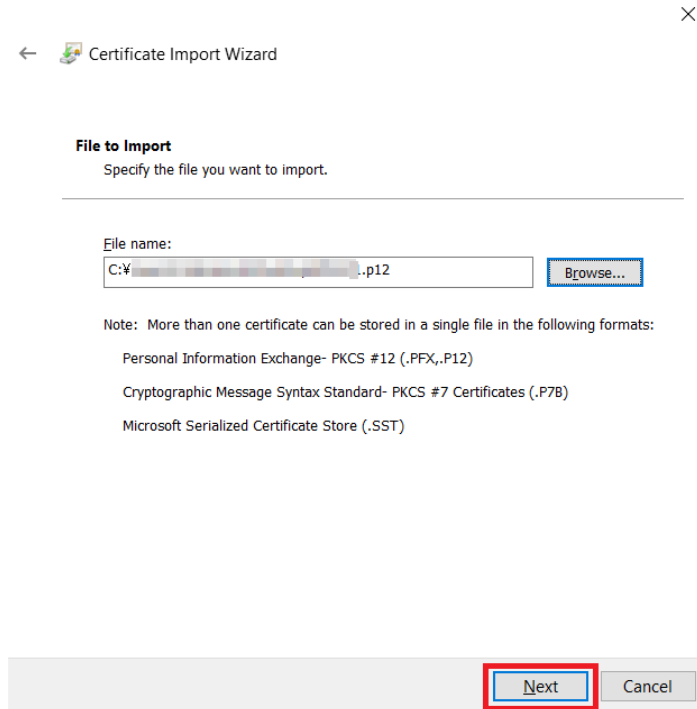
6. Change the file type to *[Personal Information Exchange(\*.pfx,\*.p12)]*.



7. Select “user account name.p12” file and click on *[Open]*.



8. After setting a file name, click on *[Next]*.



← Certificate Import Wizard

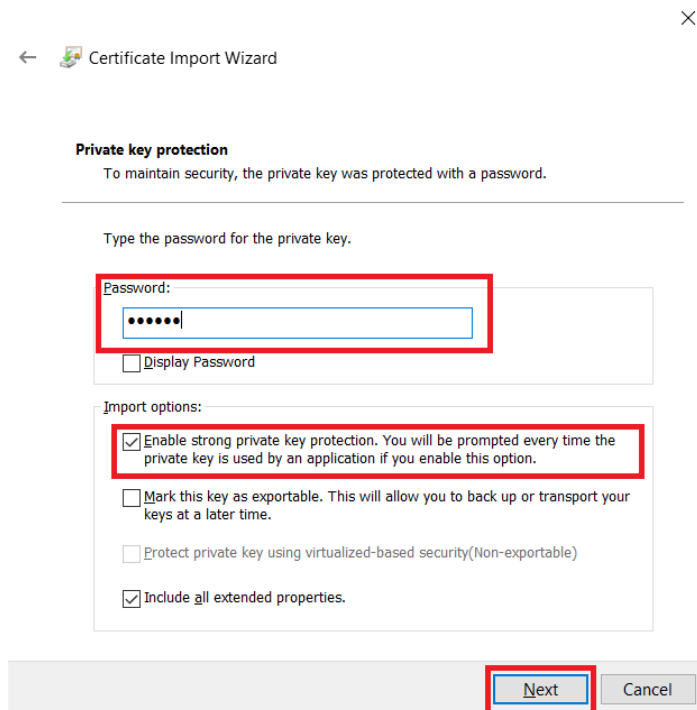
**File to Import**  
Specify the file you want to import.

File name:  
C:\¥.p12 Browse...

Note: More than one certificate can be stored in a single file in the following formats:  
Personal Information Exchange- PKCS #12 (.PFX,.P12)  
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)  
Microsoft Serialized Certificate Store (.SST)

Next Cancel

9. Input the client certificate pass phrase to *Password* and check the import option [*Enable Strong private key protection*]. then click on [*Next*].



← Certificate Import Wizard

**Private key protection**  
To maintain security, the private key was protected with a password.

Type the password for the private key.

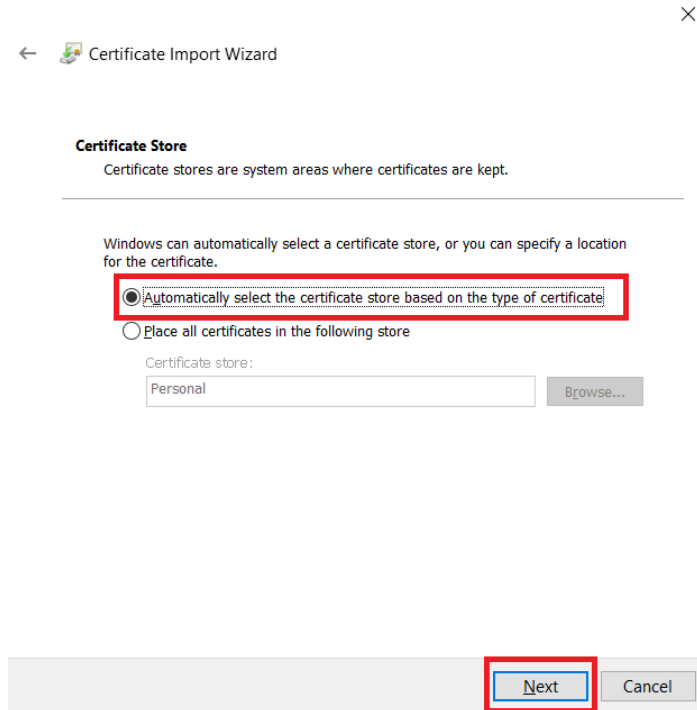
Password:  
••••• Display Password

Import options:  
☒ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.  
☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.  
☐ Protect private key using virtualized-based security(Non-exportable)  
☒ Include all extended properties.

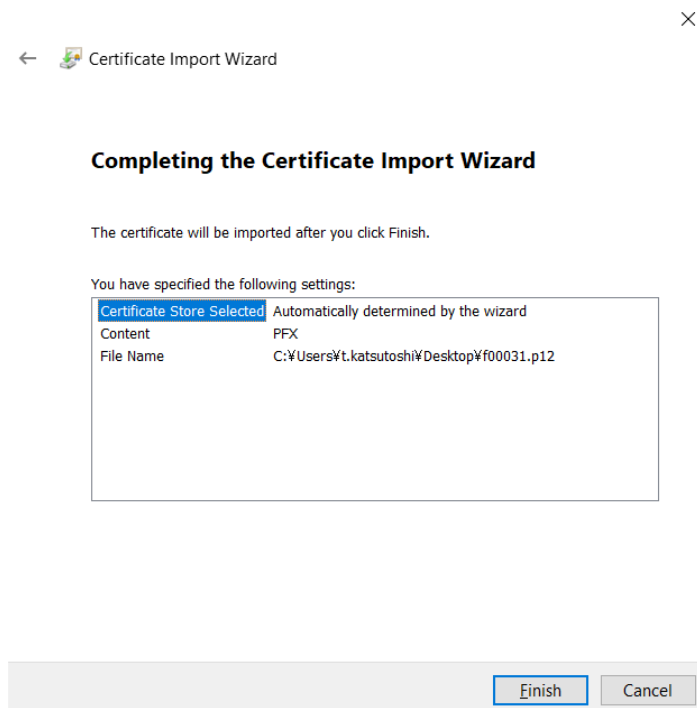
Next Cancel

**Attention:** If the client certificate pass phrase is wrong it shows an error and cannot go forward.

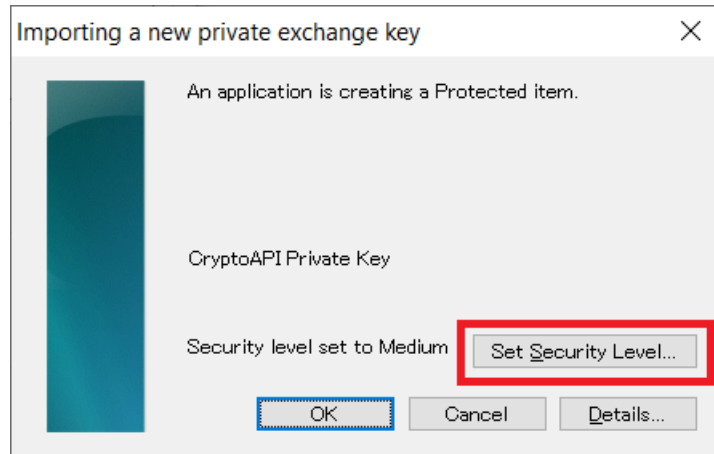
10. Check *Automatically select the certificate store based on the type of certificate* and click on [*Next*].



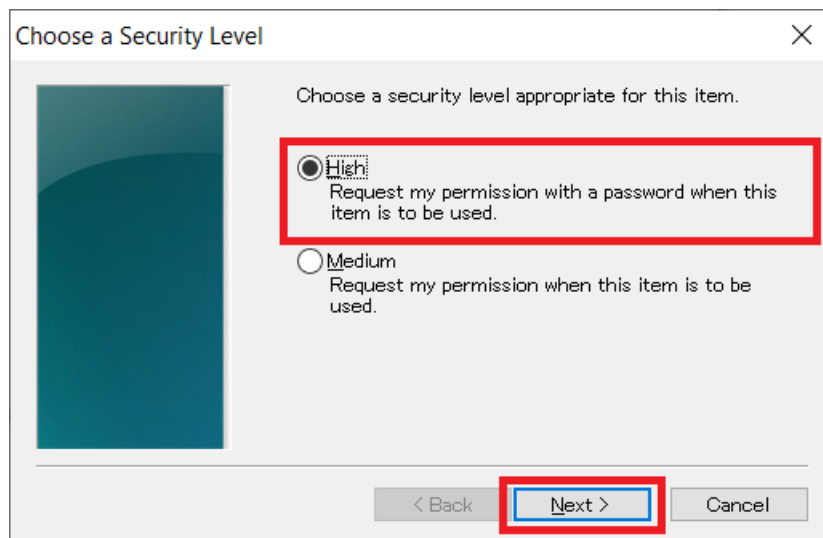
11. Click on *[Finish]*.



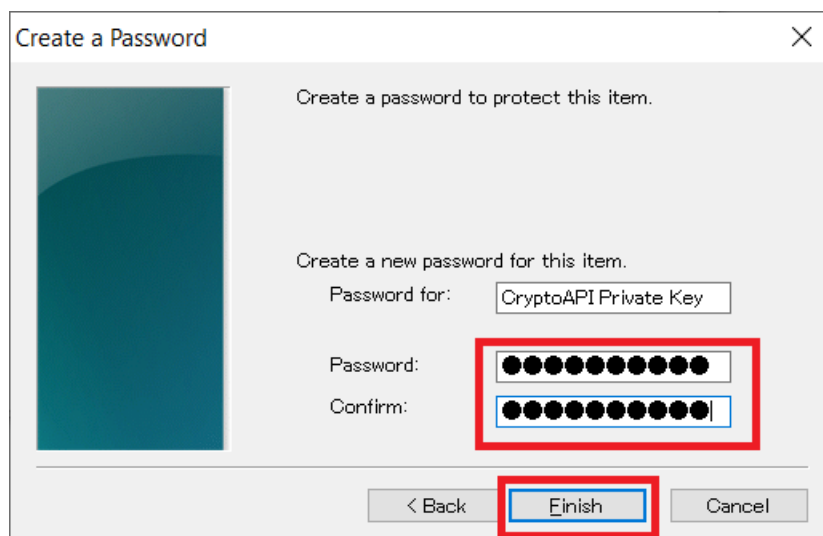
12. The “Importing a new private exchange key” screen will be displayed continuously, click on *[Set Security Level]*.



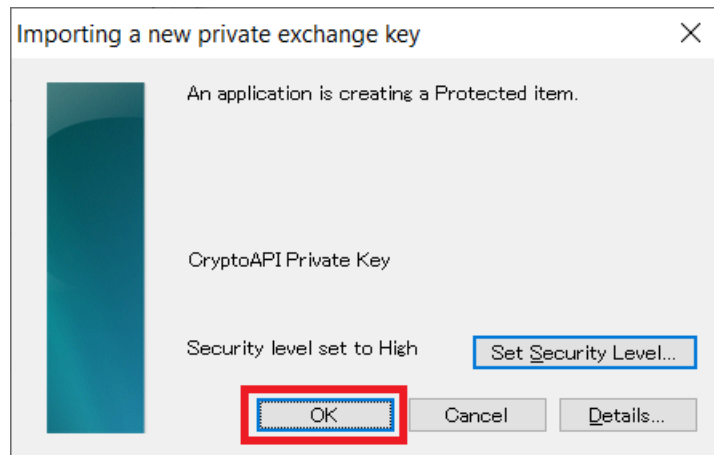
13. Check *[High]* and click on *[Next]*.



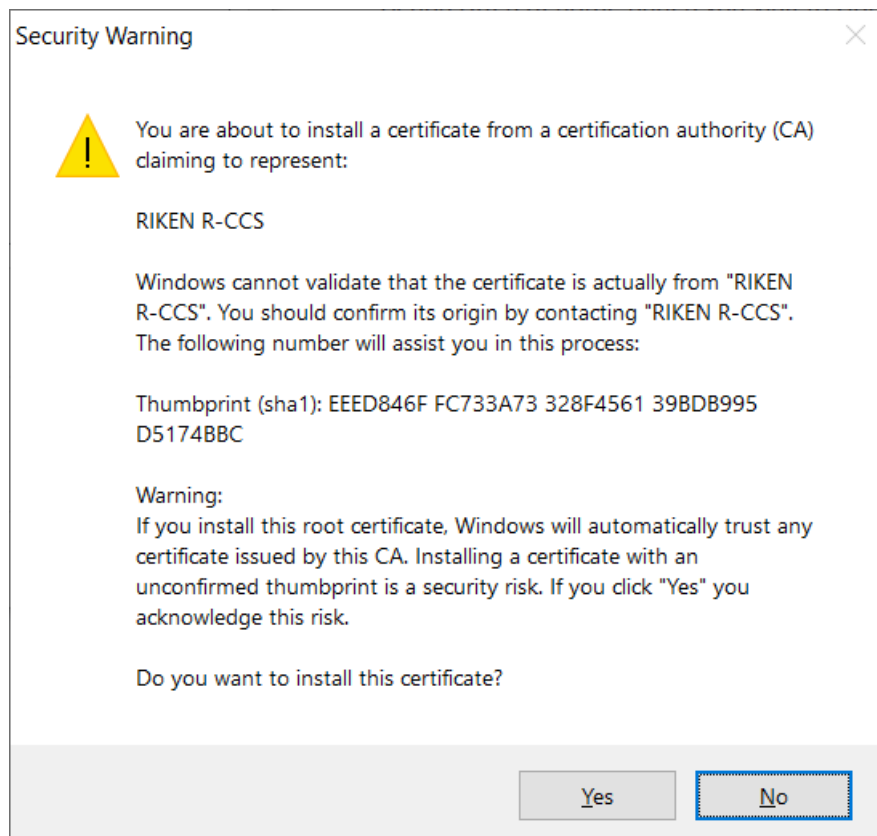
14. Set the password and click on *[Finish]*.



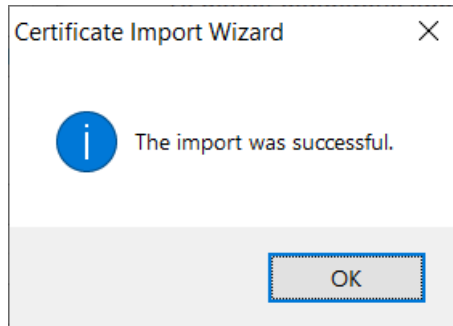
15. Click on *[OK]*.



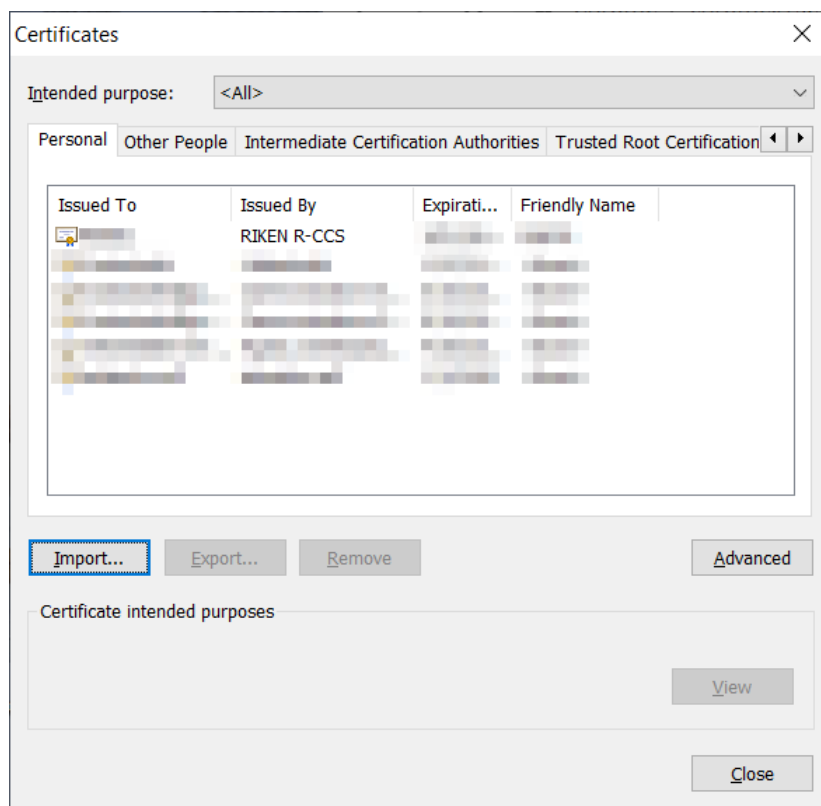
16. If a security warning is issued, confirm that the Thumbprint is (SHA-1): EEED846F FC733A73 328F4561 39BDB995 D5174BBC and click on *[Yes]*.



17. Click on *[OK]*.



18. Installation of client certificate is all done.

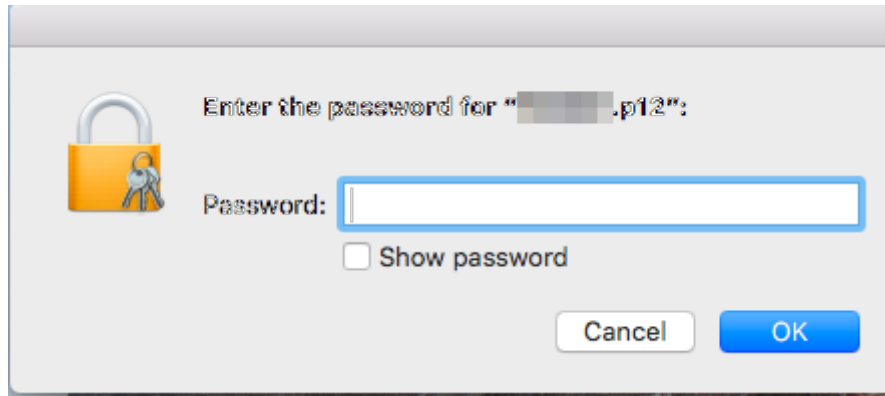


## 2.2.4 Installing the certificate to Chrome (Mac)

This indicates how to install Chrome on Mac. At macOS, the client certificate is managed at “Key chain access”.

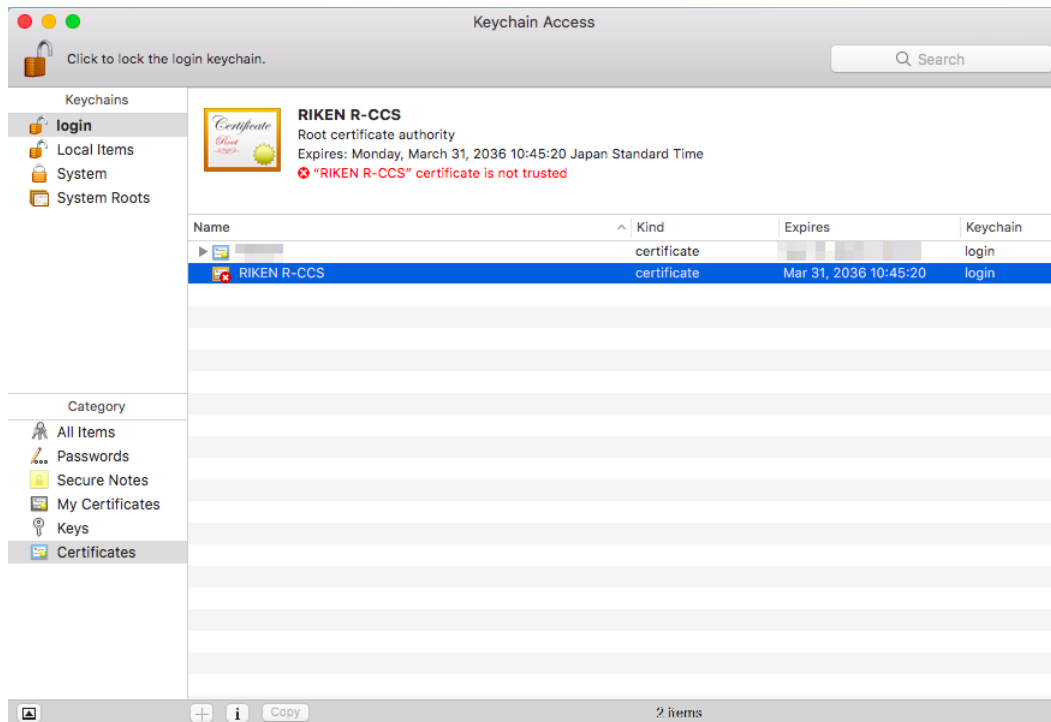
1. Client certificate: Double click “user account name.p12” file. The password input screen is show first. Enter the client certificate pass phrase and click on *[OK]*.



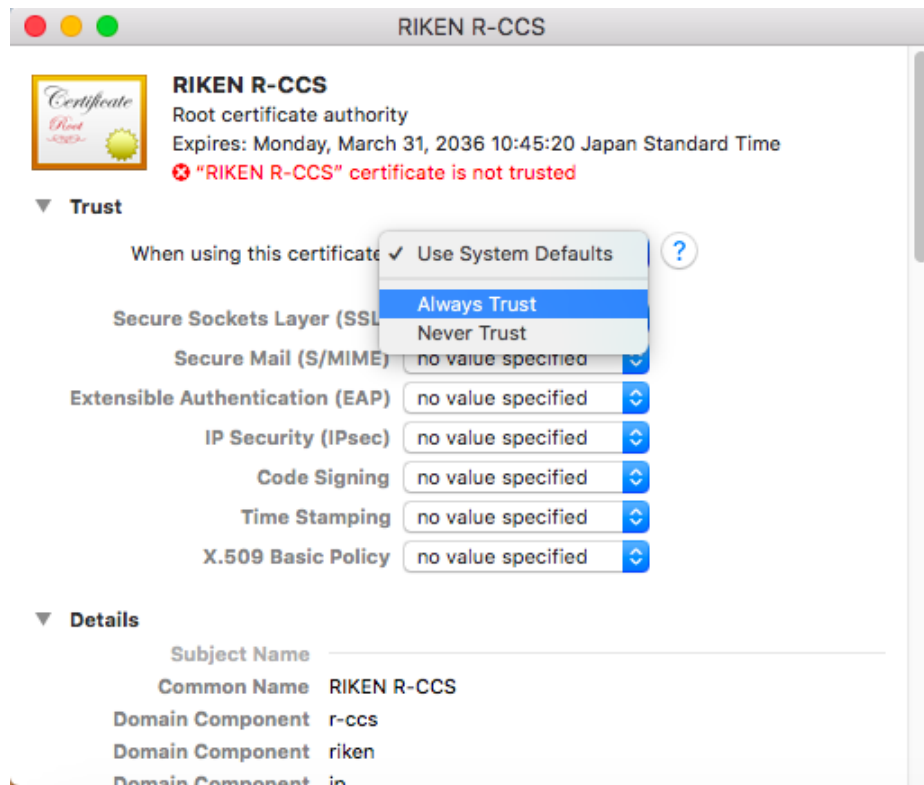


**Attention:** If the client certificate pass phrase is wrong it shows an error and cannot go forward.

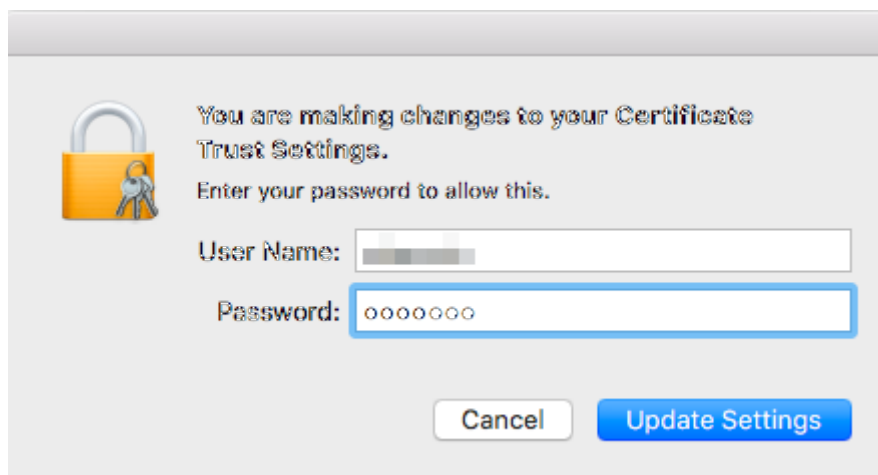
2. Open “Key chain access” screen and double click on the server certificate (RIKEN R-CCS) that issued the client certificate.



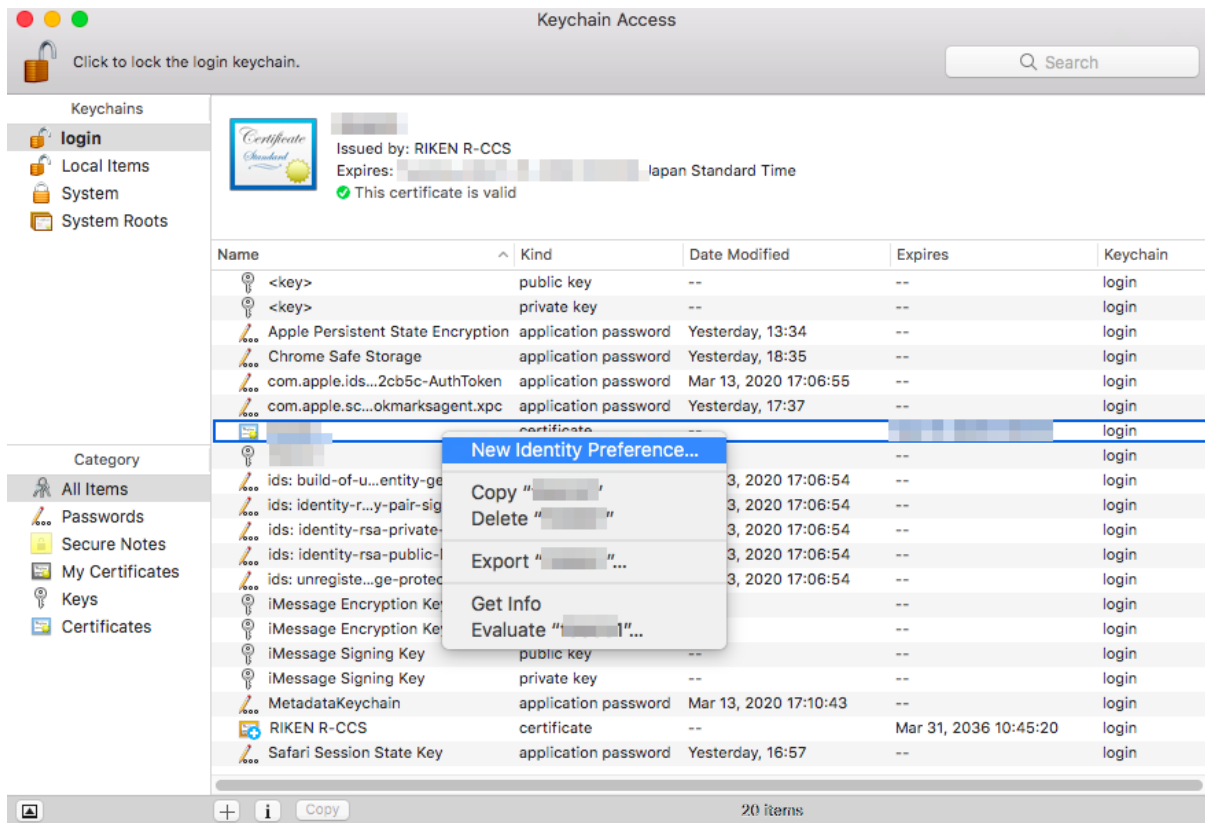
3. Click on “Route certificate authority” - “Trust” and from the list of “When using this certificate”, select “Always trust” and close the screen.



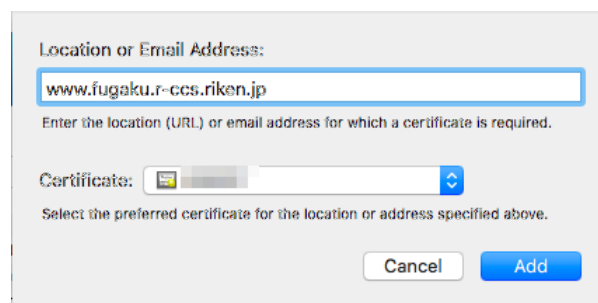
4. You will be prompted for your Mac administrator username and password to reflect the change in trust settings. Input these and click on *[Update setting]*.



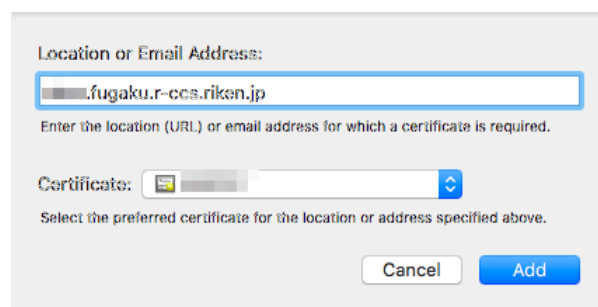
5. On the “Keychain Access” screen, hold down the Control key and click the client certificate (the local account name is shown in the name field), select *[New identify preference]*



6. To “Location or Email Address:”, input “<https://www.fugaku.r-ccs.riken.jp/>” and click on [Add].



7. With the same steps, register “<https://api.fugaku.r-ccs.riken.jp/>”.



8. Confirm if “<https://www.fugaku.r-ccs.riken.jp/>” and “<https://api.fugaku.r-ccs.riken.jp/>”’s “Identify preference” is registered to “Key chain access” and close the screen. Installation is all done.

## 2.3 Accessing steps to the user portal

This indicates how to access to the user portal.

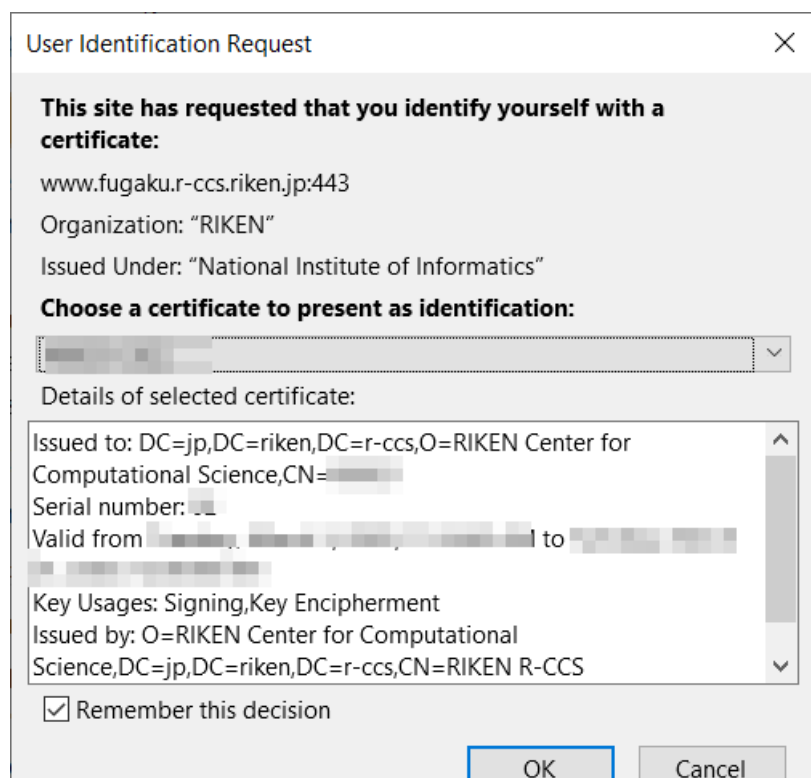
1. Open the browser and acces to the following URL.  
<https://www.fugaku.r-ccs.riken.jp/en>

### Note:

- The user portal has been tested on Mozilla Firefox and Google Chrome. If you are using other browsers and you have problems with the operation, please use a browser which operation has been confirmed. In addition, when using Microsoft Internet Explorer, it is confirmed that abnormal termination occurs with *Public key registration*.
- To prevent vulnerabilities, the user portal prohibits SSL connections and accepts only TLS 1.2 and 1.3 connections. Depending on the settings of your browser, you may not be able to connect, so please change the settings appropriately to use TLS 1.2 or later as follows.

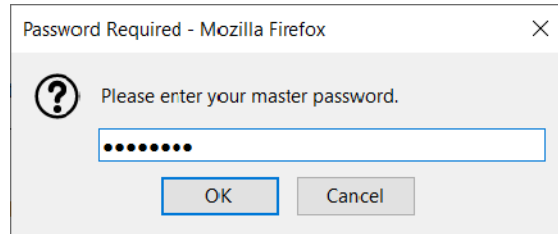
[Setting change direcion on Firefox]

1. Enter **about:config** on the address bar and press an enter key.
  2. Search with **security.tls.version**.
  3. Confirm that **security.tls.version.max** is 4 (enable by TLS 1.3).
  4. If the value is less than 4, set the value of 4.
2. Once the client certificate selection diarogue is shown, select the using local account’s client certificate.
    - The example of Firefox diarogue



3. In the password input dialog, enter the password of the private key registered when the client certificate was installed.

- The example of Firefox dialogue

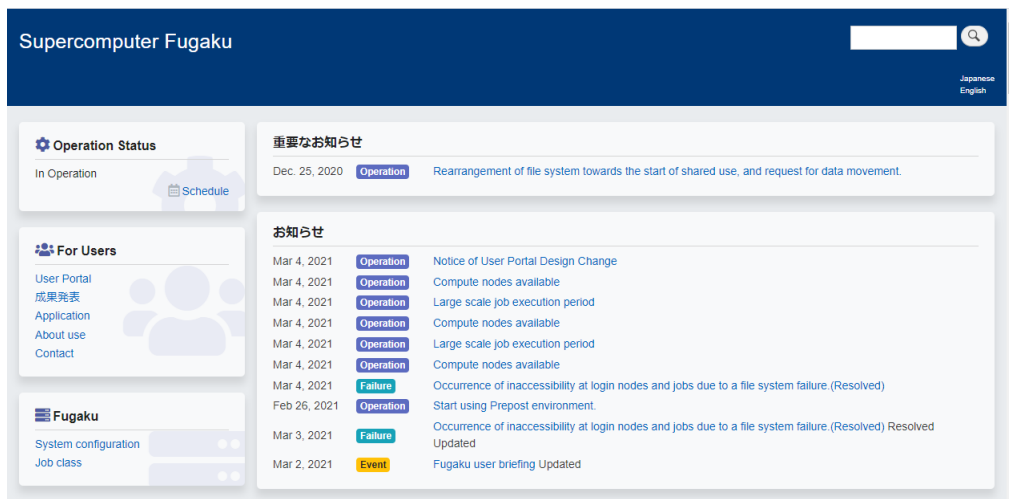


---

**Note:** If you are repeatedly prompted to enter a password for the keychain when using Chrome on your Mac, click “Always Allow” in the password input dialog.

---

4. If the client certificate is successfully authenticated, the following screen will be displayed.



## 2.4 Login

Login to Supercomputer Fugaku by using local account, logging to login node with using SSH Version2 (Public key authentication).

Create an SSH key pair (public key and private key) on the user terminal in advance and register the public key from the user portal screen. Register only the public key. When a private key is registered, processing such as temporary suspension of login may be performed as a security measure.

---

**Note:** If you change the permissions of the following directories and files under the home directory of the login node, you will not be able to login using ssh.

- home directory permission (700)
- ~/.ssh directory permission (700)

- ~/.ssh/authorized\_keys permission (600)

Do not change these permissions.

## 2.4.1 Private key/Public key creation

To use Supercomputer Fugaku, create the pair of private key and public key on the user device. Recommended creating type is from following.

- Ed25519
- ECDSA (NIST P 521)
- RSA (Key long more than 2048bit) : We plan to ban the use of RSA by the end of fiscal 2022.

This section describes the procedure for creating key pair (public key / private key) of Ed25519 using UNIX/Linux (OpenSSH) and Windows (puttygen). To use puttygen, it is necessary to install the terminal emulator PuTTY in advance.

- *Unix/Linux/Mac (OpenSSH)*
- *Windows (PuTTYgen)*

### Unix/Linux/Mac (OpenSSH)

Execute a command **ssh-keygen** on the user's device, create a private / public key pair.

1. Start terminal and execute a command **ssh-keygen**.
  - If Mac(OS X), start Terminal(*Application* → *Utility* → *Terminal*) and execute a command **ssh-keygen**.
  - If UNIX/Linux, start terminal emulator and execute a command **ssh-keygen**.

```
[terminal]$ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/user_name/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase): # Enter passphrase
Enter same passphrase again: # Re-enter the same passphrase
Your identification has been saved in /home/name/.ssh/id_ed25519.
Your public key has been saved in /home/name/.ssh/id_ed25519.pub.
The key fingerprint is:
SHA256:khhWyIyUqMnyjK10k7818EivKbQLNgP3vyhjYBgviF8 namehostname
The key's randomart image is:
+--[ED25519 256]--+
|    ...          |
|    ...+ o       |
|.o    . * .      |
|= .    . o       |
|= @    + S       |
| @o%    . .      |
|= % . =         |
| * = 0 =        |
| + = + = E o .   |
+-----[SHA256]-----+
```

**Note:**

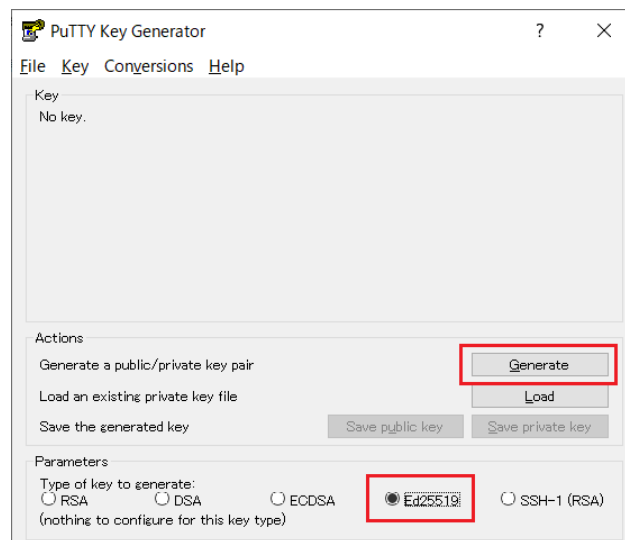
- Set a passphrase that is difficult for others to guess, just like a password. Please be sure to set a passphrase. We recommend a passphrase length of at least 15 characters.

2. Once execute **ssh-keygen**, two types are created: a private key (id\_ed25519) and a public key (id\_ed25519.pub) on .ssh directory under the home directory.  
Register the public key (id\_ed25519.pub) using the user portal.

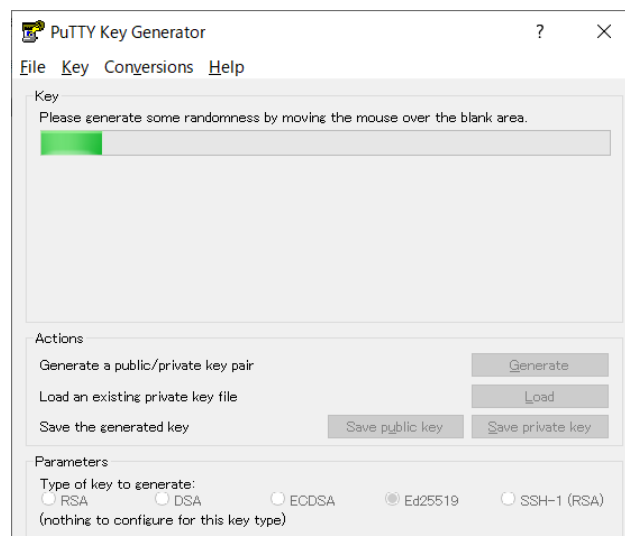
## Windows (PuTTYgen)

Create a private / public key that can be used with PuTTY / WinSCP with puttygen.

1. Start puttygen.  
Select “Ed25519” for Type of key to generate, then click “Generate”.



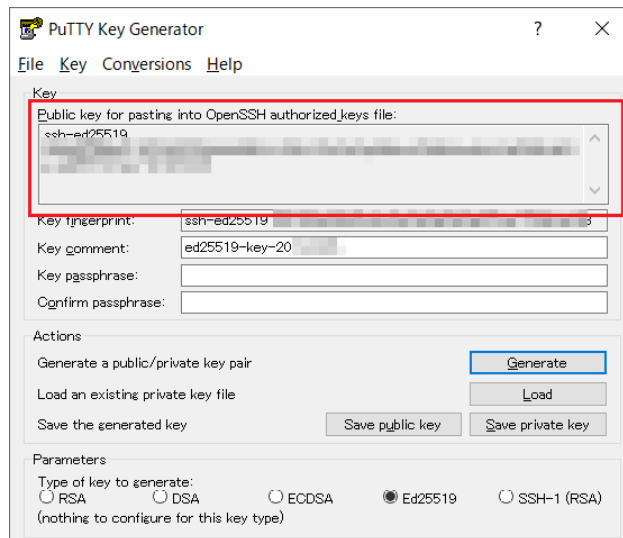
2. Move the mouse cursor randomly.



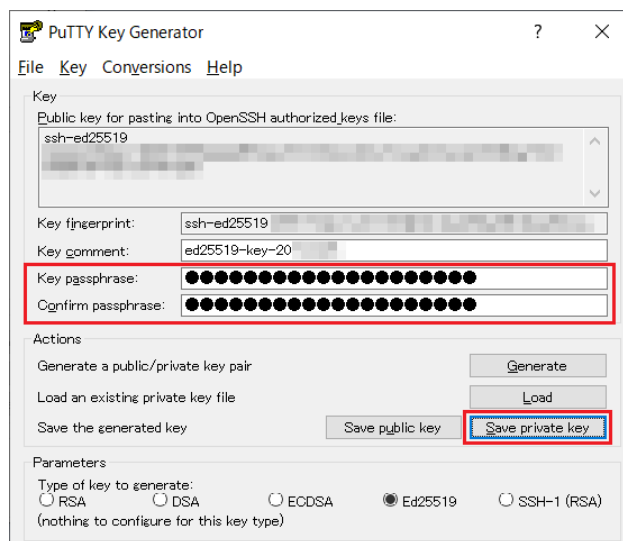
3. Save the public key.

Copy the displayed contents on “Public key for pasting in to OpenSSH authorized\_keys file:” to the clip board (It is recommended to paste on the notepad).

Register the contents pasted on the clip board (Public key) using the user portal.



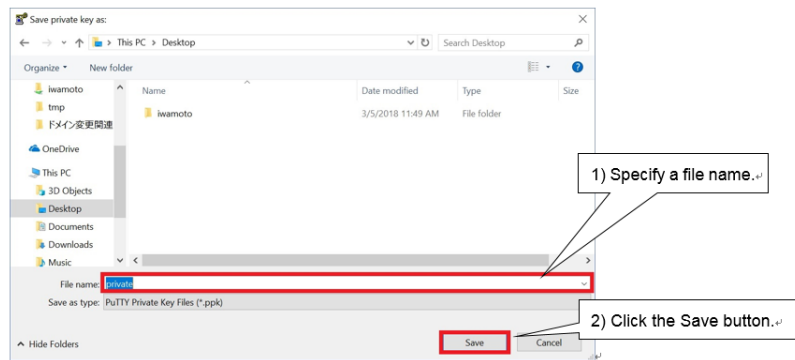
4. Input a passphrase to both “Key passphrase” and “Confirm passphrase”. After inputting, click “Save private key” and save the private key. Remember your passphrase because it is required to log in to the login node.



**Attention:** Set a passphrase that is difficult for others to guess, just like a password. Please be sure to set a passphrase. We recommend a passphrase length of at least 15 characters.

5. Input a file name for storing the private key to “File name(N)”, click “Save(S)”. The private key is stored.



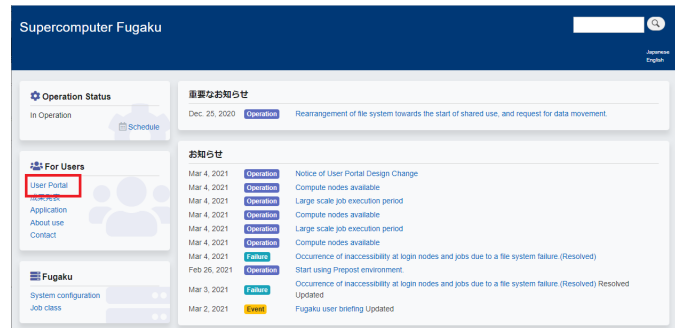


## 2.4.2 Public key registration

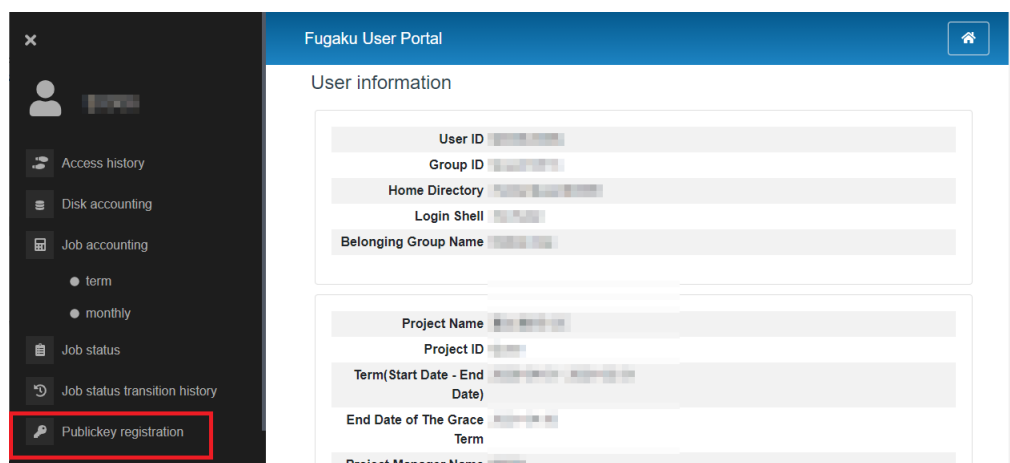
- *Registration using user portal*
- *Additional registration of public key*

### Registration using user portal

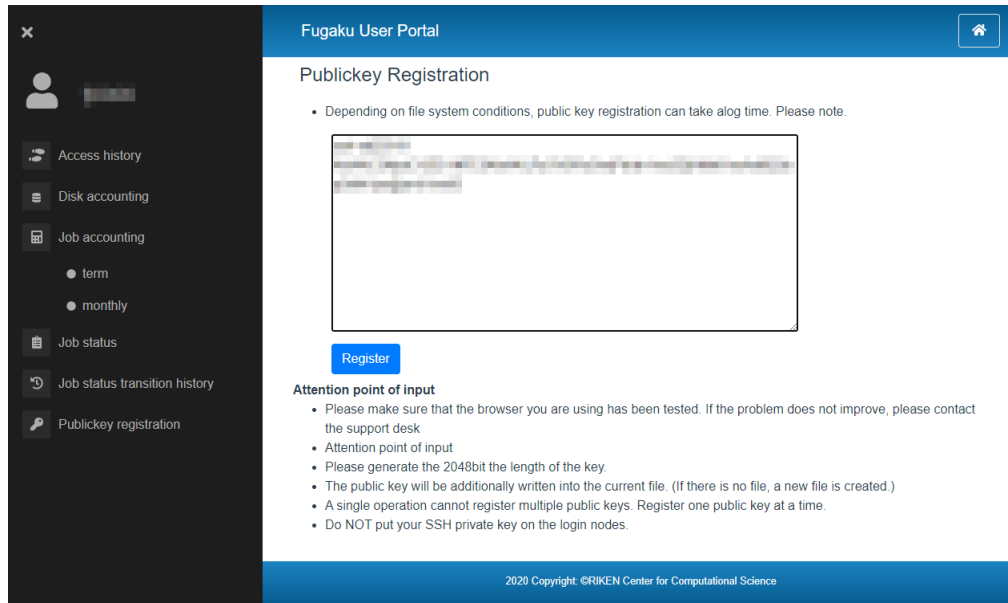
1. Log in to the user portal(<https://www.fugaku.r-ccs.riken.jp/en>), then click [User Portal] from menu.



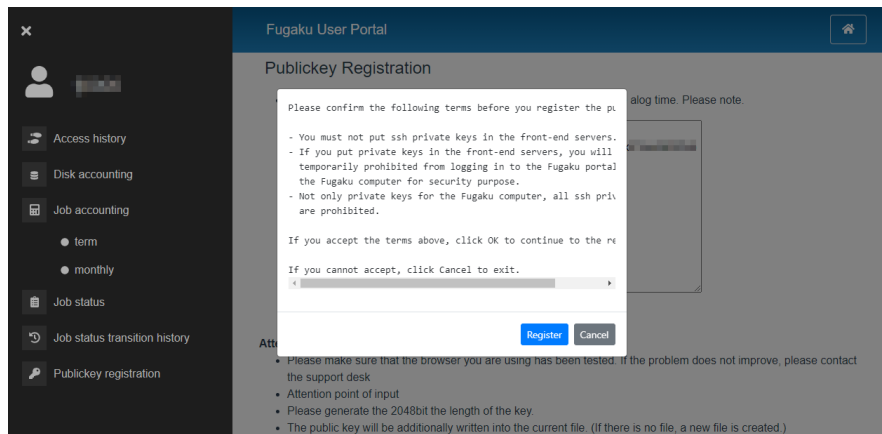
2. Click [Publickey registration] from menu.



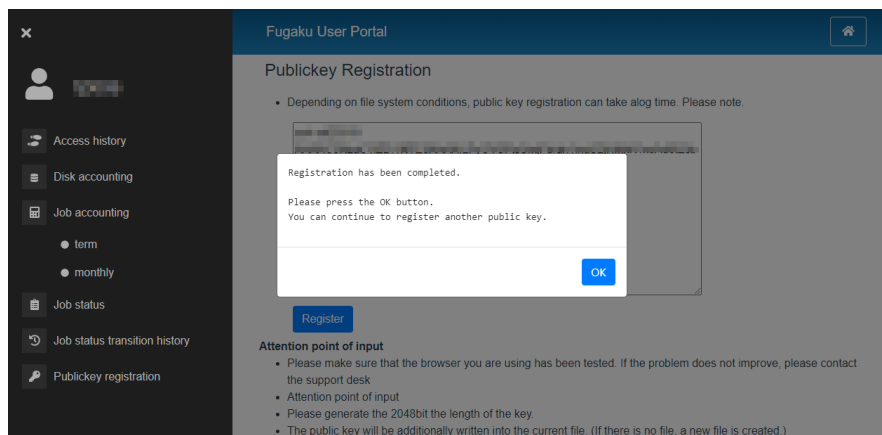
3. Copy and paste the public key to be used to “Publickey registration” area.



4. Click [Register].
5. Confirm the contents, then click [Register].



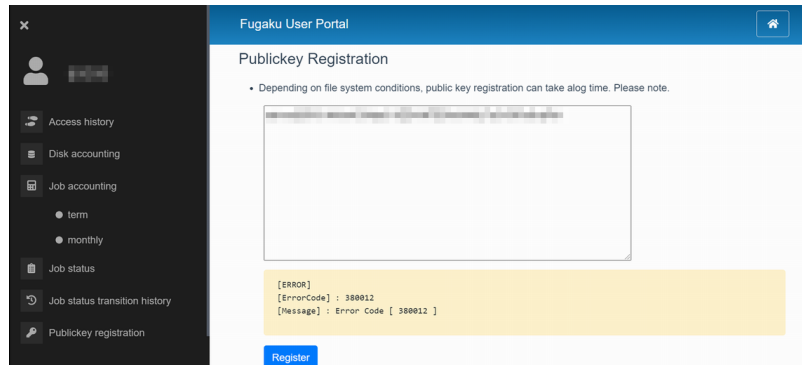
6. "Registration has been completed." is displayed on the screen, then the public key registration process is completed.



**Note:** Only one public key can be registered per operation. For the second and subsequent operations,

additional registration is required. If you want to register two or more public keys, repeat the same operation.

7. Error message will be shown if the registered public key is not correct. Confirm the public key and proceed the operation again.



### Additional registration of public key

This section describes the procedure for registering additional public keys in the login node.

There are a method of registering additionally using the user portal and a method of editing the file directly by logging in to the login node. This section shows how to edit a file on the login node.

1. Edit `~/.ssh/authorized_keys` on login node.

```
[_LNlogin]$ vi ~/.ssh/authorized_keys
```

Press [i] key to enter vi editor insert mode.

Click the right mouse button and paste the contents of `.ssh / id_rsa.pub`.

Press the [esc] key, enter [wq!], and press the [Enter] key.

2. Change permission of private key registered `authorized_keys`.

```
[_LNlogin]$ chmod 600 ~/.ssh/authorized_keys
```

### 2.4.3 Accessing direction

This indicates how to access to Supercomputer Fugaku.

To login to the login node, execute the steps of “*Private key/Public key creation*” and it is required that the public key is registered to login node.

Program development (Creating program/Compiling) and job controlling (Job submission/Job status display/Job deleting) are proceeded from login node.

- *Login node*
- *Login node (PuTTY)*

## Login node

Access by the following host name from the user device

Host name : login.fugaku.r-ccs.riken.jp

This indicates the execution example of **ssh** command.

[Public key authentication]

```
[terminal]$ ssh user_name@login.fugaku.r-ccs.riken.jp
The authenticity of host 'XXXXXX (nnn.nnn.nnn.nnn)' can't be established.
XXXXX 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 # Enter yes (Initial)
Enter passphrase for key '/home/group_name/user_name/.ssh/id_rsa': # Enter pass-phrase
[_LNlogin]$
```

1. ssh l00504@login.fugaku.r-ccs.riken.jp  
2. yes  
3. hcq33\*\*\*7

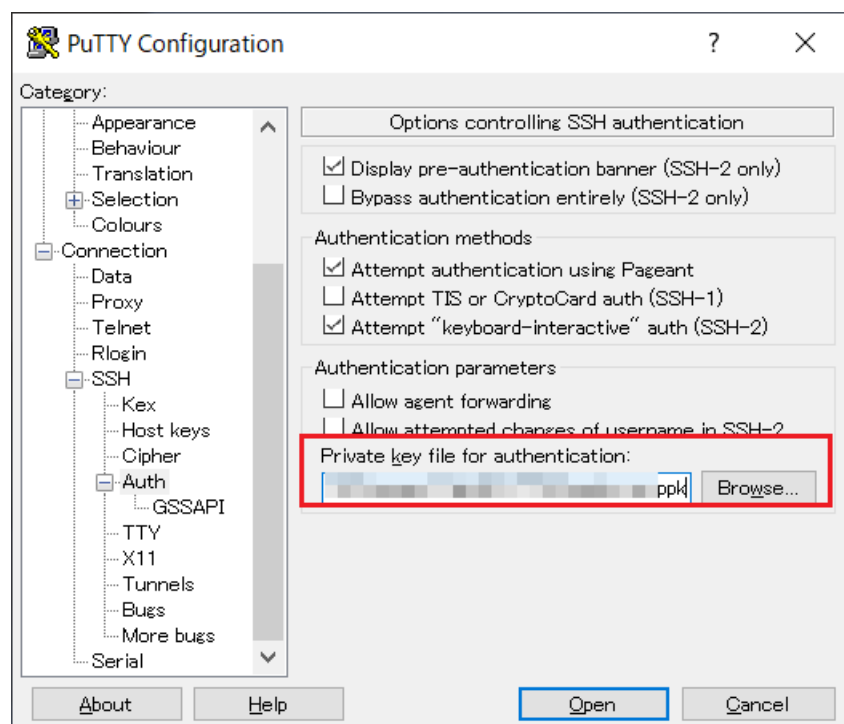
把每个的登录名id\_rsa改成简单的登录名  
1. vi ~/.bash\_profile  
2. 加上 alias fugaku\_qiu="ssh l00504@login.fugaku.r-ccs.riken.jp"  
3. source ~/.bash\_profile  
4. qiu to login the login node

1. When the first login in, the confirmation message about registering the host key (Are you sure you want to continue connecting) is displayed. Enter “yes”.
2. Specify **ssh**'s option **-X** to enable X11 Forwarding function when connecting to the login node.
3. Specify **ssh**'s **-A** to enable SSH Agent-forwarding function when connecting to the login node.
4. Operating the multiple device's login node. About home area (/home) and deta area (/data), share with the each login node. It is the same with the language software environmet.

## Login node (PuTTY)

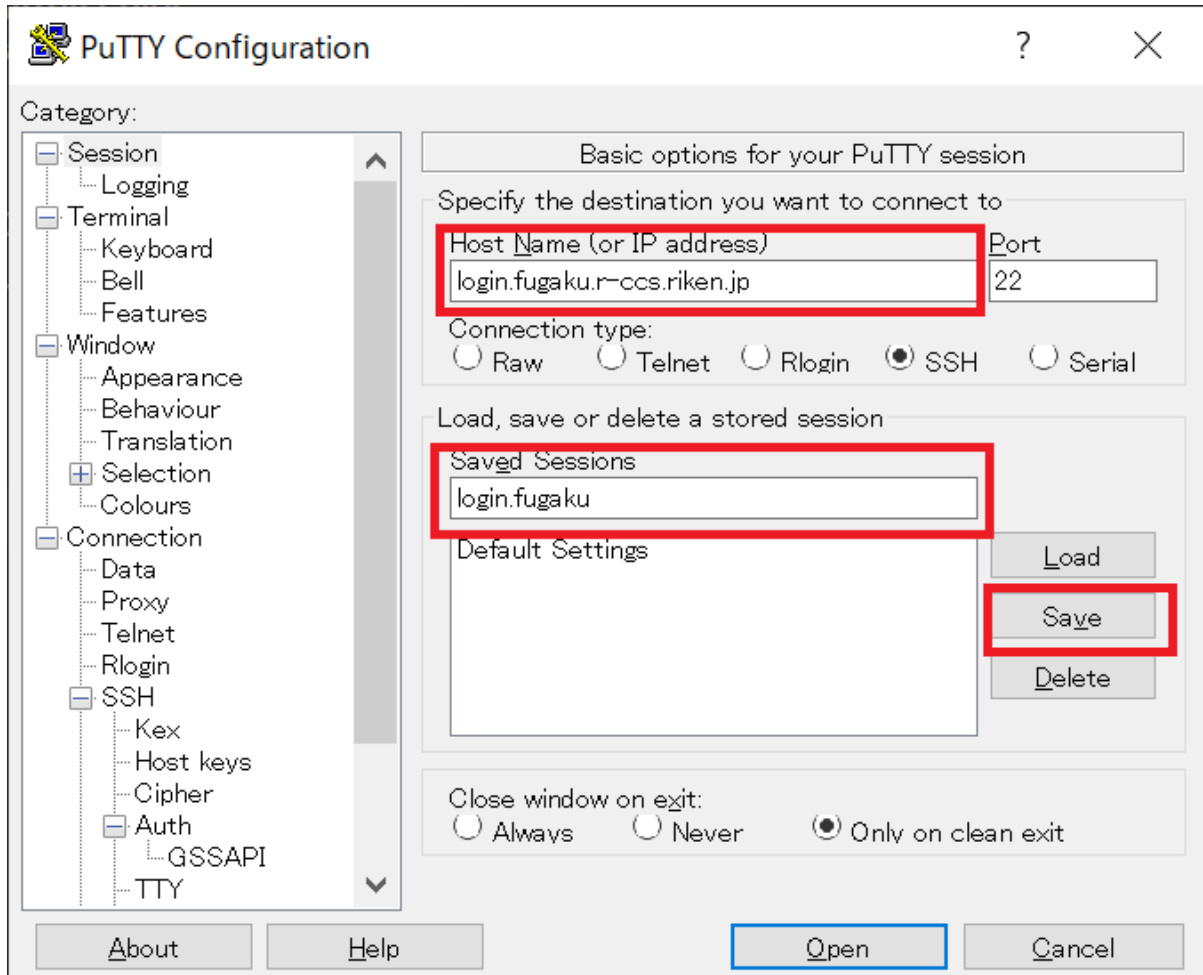
This indicates how to login to the login node with using Windows (PuTTY).

1. Start PuTTY. Set the private key which stored in the user device.  
Click on [Browse] from [Connection] → [SSH] → [Auth].  
Select the pribate key created with puttygen.

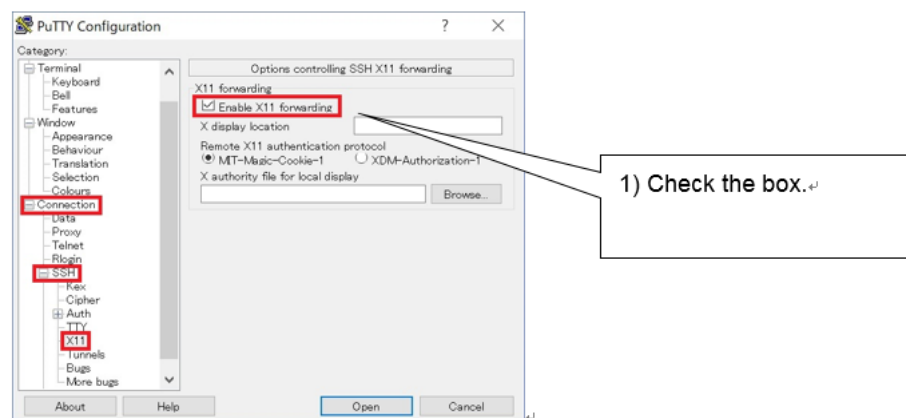


2. Select [Session].

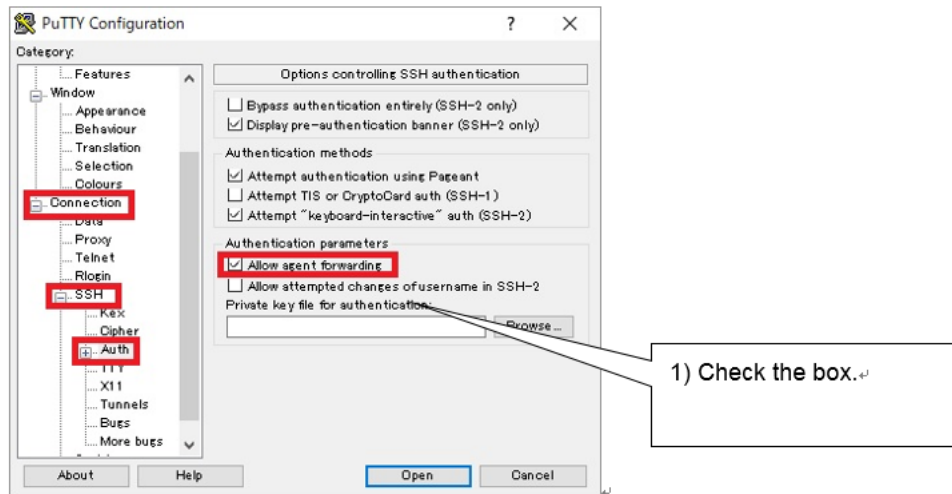
To [Host Name(or IP address)], enter login node host name. To save the set contents, input the name to save to [Saved Sessions] and click on [Save]. From the second logging in, select the saved name and click [Load].



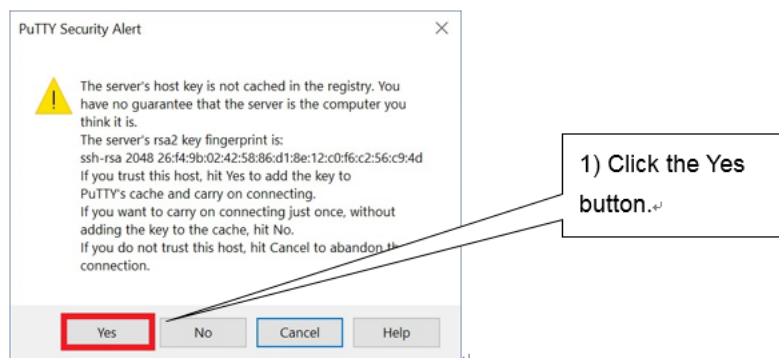
3. To enable X11 forwarding function when connecting to the login node, before click [Open], open [Connection] → [SSH] → [X11] and put the check to [Enable X11 forwarding].



4. To enable Agent-forwarding function when connecting to the login node, before click *[Open]*, open *[Connection]* → *[SSH]* → *[Auth]* and put the check to *[Allow agent forwarding]*.



5. Click on *[Open]*. It starts connecting to the login node.
6. When the first login, about the host key registration, the confirmation screen will be shown. Click on "Yes(Y)".



8. Input local account name and pass phrase and logging to the login node.

```
login as: user_name # Enter a local_
↪account
Authenticating with public key "imported-openssh-key"
Passphrase for key "imported-openssh-key": passphrase # Enter a pass_
↪phrase
Last login: Tue Mar 27 09:57:12 2018 from xxx.xxx.xxx.xxx
login$
```

## 2.4.4 File transfer method

Files can be transferred via the login node using the file transfer program (scp/sftp) installed on the user terminal. You can use `login.fugaku.r-ccs.riken.jp` for transfer.

Use of protocols (ftp/r commands) that are vulnerable to security is prohibited.

For file transfer, the procedure for “*Private key/Public key creation*” must be performed, and the public key must be registered on the login node.

- *File transfer (sftp)*
- *File transfer (scp)*
- *Windows (WinSCP)*

### File transfer (sftp)

#### 1. sftp command execution example

```
[terminal]$ sftp user_name@login.fugaku.r-ccs.riken.jp
Enter passphrase for key '/home/group_name/user_name/.ssh/id_rsa': # input_
↪passphrase
sftp>
```

#### 2. File transfer example (put)

```
sftp> put a.f90
Uploading a.f90 to /home/group_name/user_name/a.f90
sample.f90                                100%   18    0.0KB/s  ↪
↪00:00
sftp>
```

#### 3. File transfer example (get)

```
sftp> get sample.sh.o9110
Fetching sample.sh.o9110 to /home/group_name/user_name/sample.sh.o9110
sample.sh.o9110                          100%   18    0.0KB/s  ↪
↪00:00
sftp>
```

### File transfer (scp)

#### 1. scp example of command execution is shown below. (From terminal to login node)

```
[terminal]$ scp local_file user_name@login.fugaku.r-ccs.riken.jp:remote_
↪file
Enter passphrase for key '/home/group_name/user_name/.ssh/id_rsa': # ↪
↪Input passphrase
[terminal]$
```

#### 2. scp example of command execution is shown below. (Login node to terminal)

```
[terminal]$ scp user_name@login.fugaku.r-ccs.riken.jp:remote_file local_
↪file
Enter passphrase for key '/home/group_name/user_name/.ssh/id_rsa': # ↪
↪Input passphrase
```

(continues on next page)

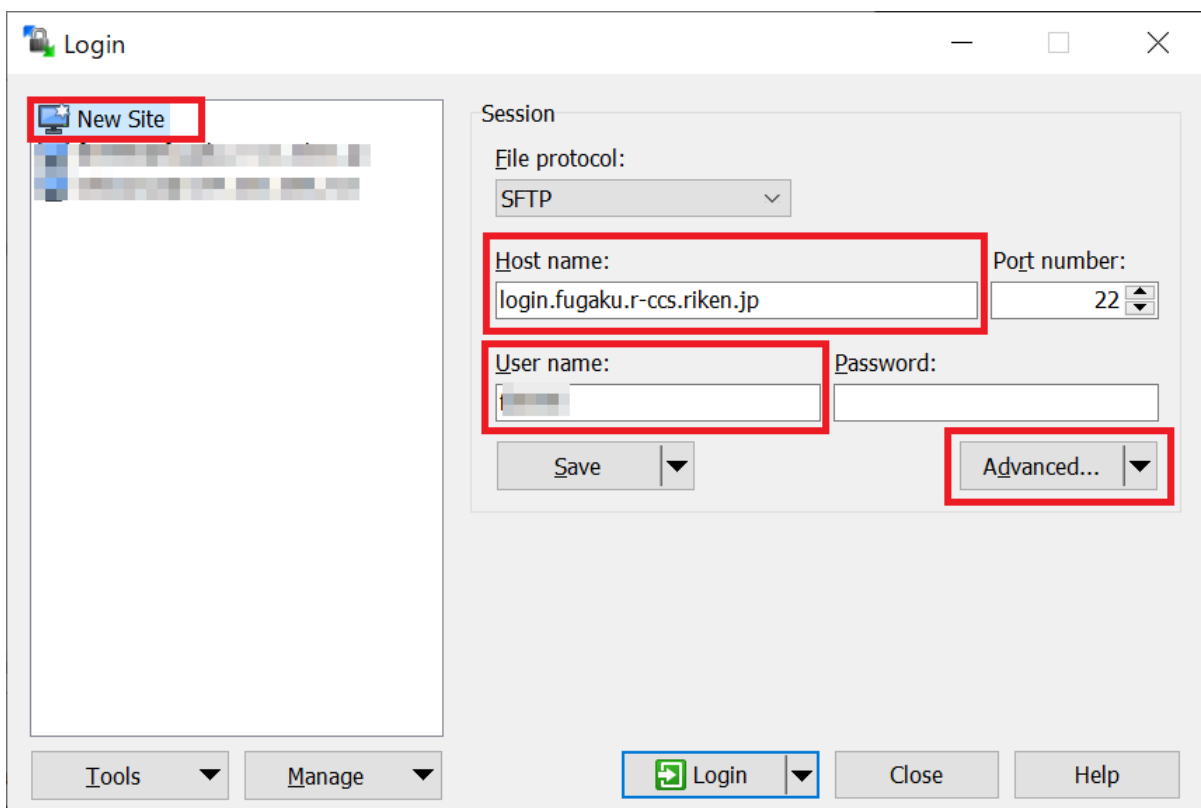
(continued from previous page)

```
[terminal]$
```

## Windows (WinSCP)

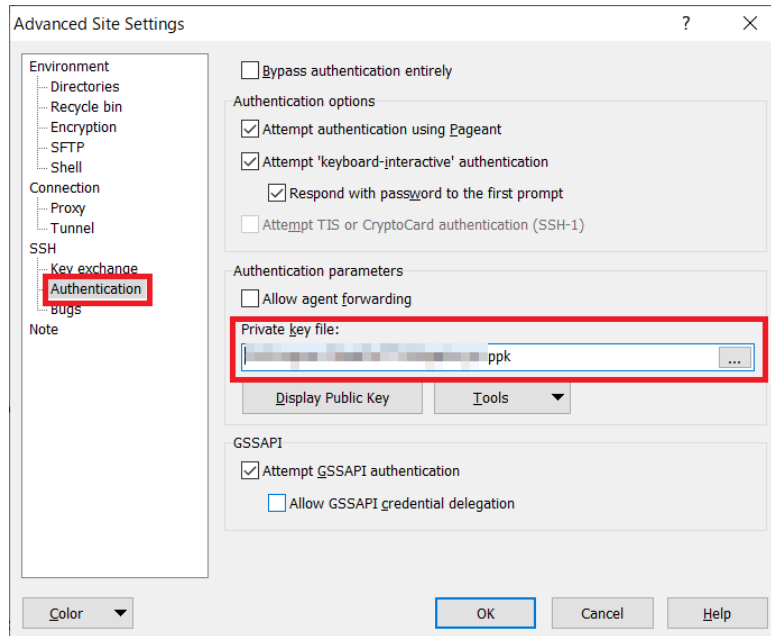
For Windows, use a file transfer program such as WinSCP to transfer the file to the login node. An example of connection with WinSCP is shown below.

1. Start WinSCP and select *[New Site]*.
2. Enter the host name of the login node (`login.fugaku.r-ccs.riken.jp`) to “*Host name*”.
3. Enter the user name to “*User name*”.
4. Click *[Advanced...]*.

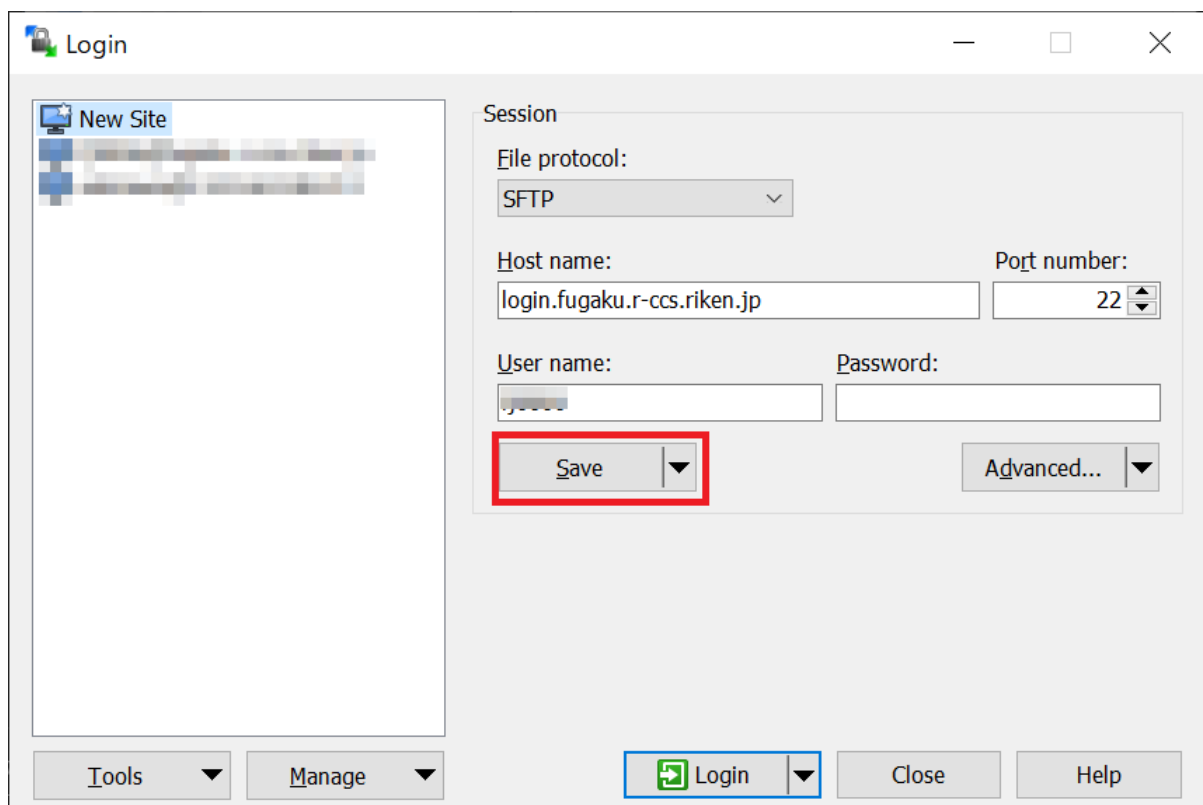


5. Set the private key file's name of putty in *[Private key file]* of *[Authentication]*, then click *[OK]*.

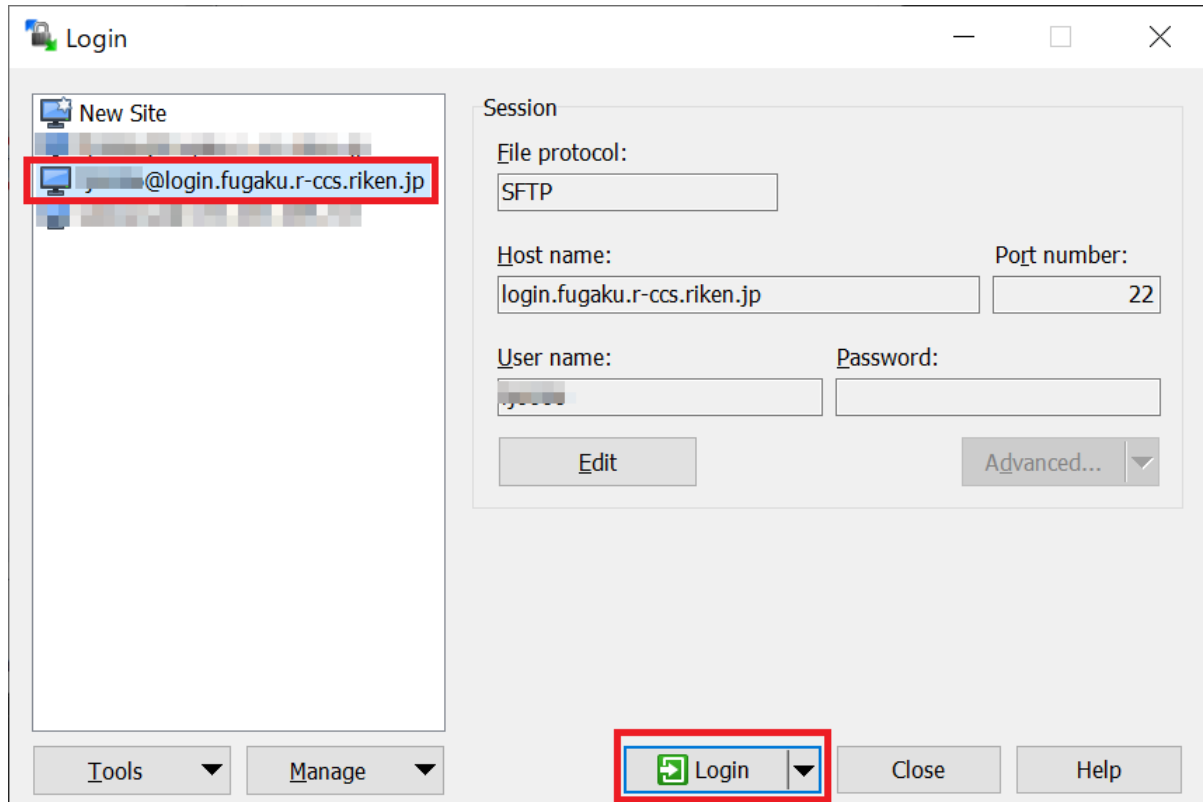




6. Click *[Save]* and save the settings.



7. Select the saved setting, then click *[Login]* to connect.



8. After the connection is completed, a screen similar to explorer will be displayed, and you can transfer files by dragging and dropping them.

## 2.4.5 Login shell

Login shell is `/bin/bash`.

## 2.4.6 E-mail distribution of Fugaku operation information

An operation information mail is delivered to Fugaku account (uid).

In order to receive the mail, the user must register the forwarding destination mail address. (If you do not register, the mail is discarded.)

We will send you an email about the following operation information. The content of distribution will be gradually expanded.

- Information of jobs affected by a system failure.
- Operation information
- Others

[How to register your e-mail address]

Create a “`.forward`” file in the user’s home directory and register the email address that you want to receive. Examples of “`.forward`” and filtering configurations will be in the [FAQ](#).

```
[_LNlogin]$ vi ~/.forward
*****@*****.com          chuanqiuhe@gmail.com
```