

Agenda

Part I

basic information about
HPC resources

09:00 - 09:05	Welcome	Tim Cramer
09:05 - 09:35	HPC Architecture Basics and RWTH Resources	Tim Cramer
09:35 - 10:05	Storage Strategy for HPC Users	Philipp Martin
10:05 - 10:10	Break	
10:10 - 10:55	NHR and RWTH Computing Projects	Tim Cramer
10:55 - 11:30	Introduction to JupyterHub	Alvaro Frank
11:30 - 12:00	Access to CLAIX and Using multi-factor Authentication	Tim Cramer
12:00 - 13:00	Break	

Part II

basic information about
HPC usage

13:00 - 13:30	Cluster Software Environment HPC	Felix Tomski
13:30 - 13:50	Container Usage	Sven Hansen
13:50 - 14:30	Introduction to Slurm	Alvaro Frank
14:30 - 14:45	Break	
14:45 - 15:30	Parallel Programming Overview	Tim Cramer
15:30 - 16:15	Performance Metrics & Measurements	Felix Tomski
16:15 - 16:30	Closing Session	Tim Cramer



Access to CLAIX and Using multi-factor Authentication

Tim Cramer

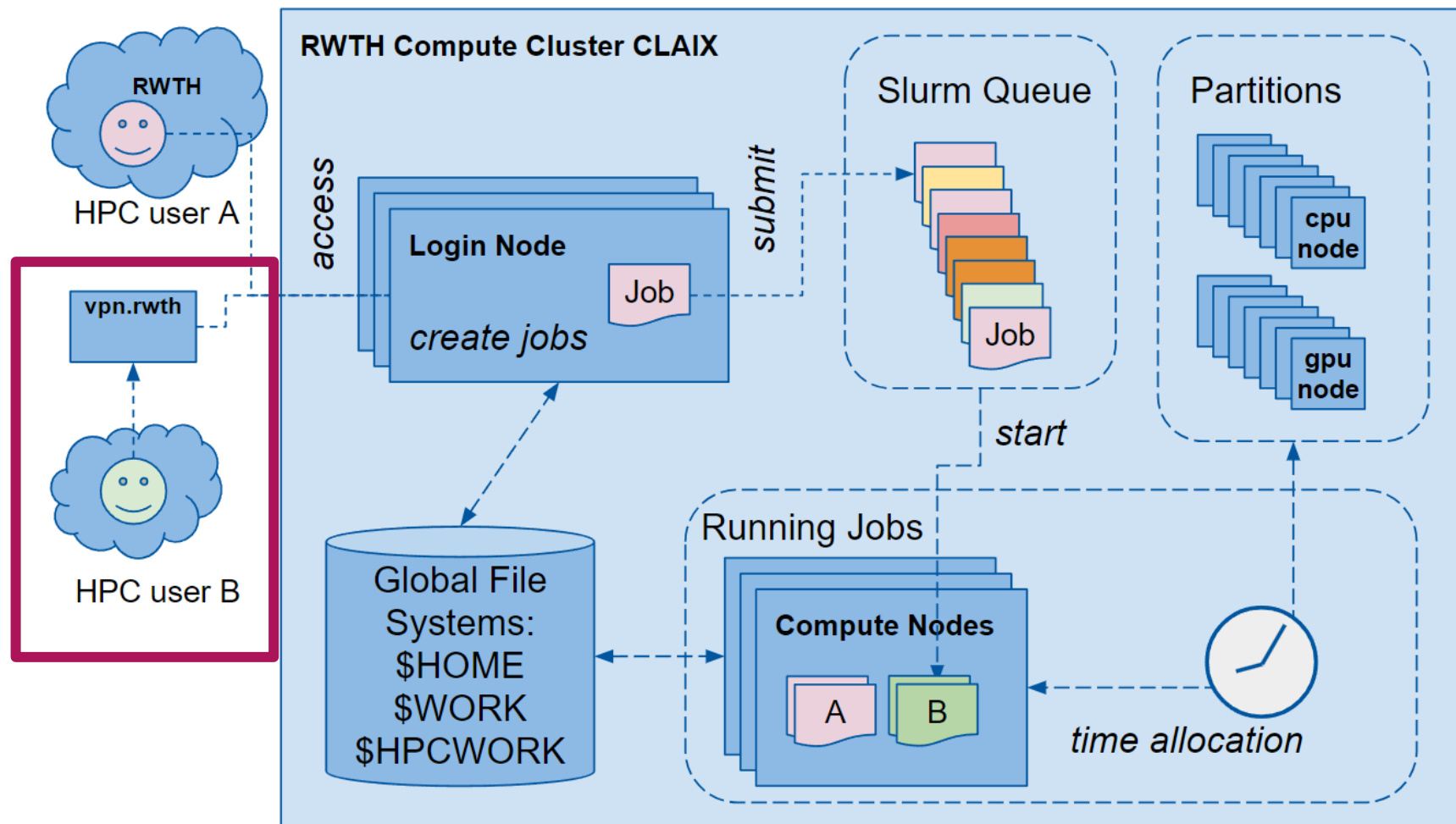
Using Your HPC Account: Requirements

Recap: Who can use the computing resources at RWTH Aachen University?

- Authorized users without computing project application
 - Members of RWTH Aachen University
 - Members of the UKA for research and teaching (FB10)
 - Persons with partner status of RWTH Aachen University
- Authorized users through JARDS computing project application
 - Members of German public or government-approved teaching and research institutions
 - Members of non-university research institutions need a PI who owns a Ph.D. / professorship from a German university
 - Members of non-university research institutions are still welcome as project members (PMs)
- Projects require a Principle Investigator (PI)
 - Leading researcher (usually with doctorate)
- Citizens of countries that are subject to the export control policy of the German Federal Government may need additional authorization from the German Federal Office for Economic Affairs and Export Control (BAFA) before they are allowed to use HPC resources

Exception: RWTH projects for members of FZJ

CLAIX Usage - Overview



- Getting Started Guide
- Firewall: Use VPN if outside of RWTH and other trusted (university) networks
 - Cisco Any Connect
 - DFN Network
 - FZ Jülich
 - TU Darmstadt
- RWTH IDM Account

Getting Started Guide

<https://help.itc.rwth-aachen.de/service/rhr4fjjuttf/article/b7221149cca349e196cc0a28fcb a8cc9/>

VPN

<https://help.itc.rwth-aachen.de/service/vbf6fx0gom76/>

IDM Account

<https://idm.rwth-aachen.de/HomePage>

- Create account / set password via RegApp
 - **Selfservice portal for HPC accounts**
 - Register for the service
 - Change your HPC account password
 - Upload and manage SSH keys
 - Registering tokens for multi-factor authentication (**mandatory after January, 15th 2024**)
 - <https://regapp.itc.rwth-aachen.de/>

Using Multi-Factor Authentication on CLAIX

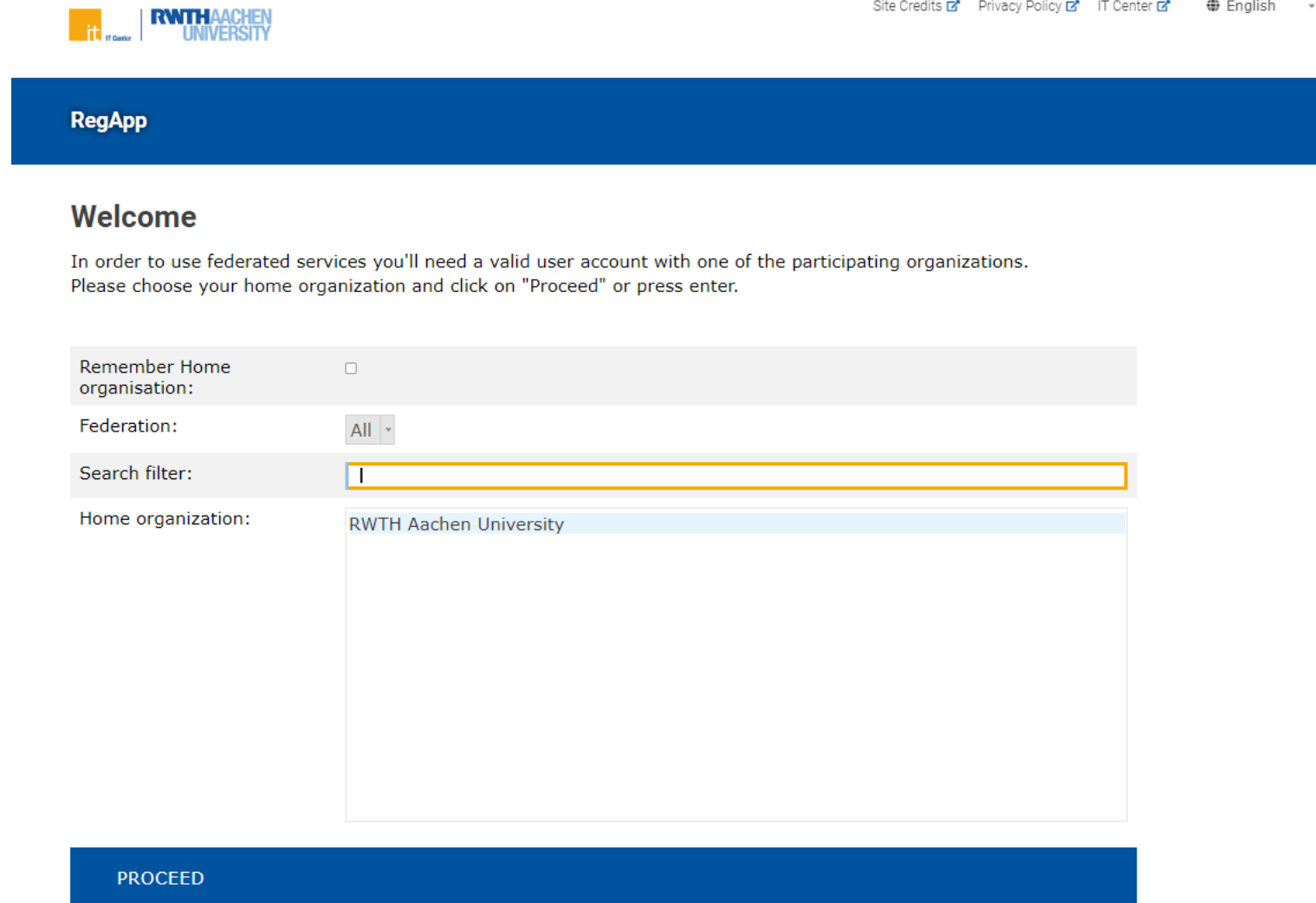
- What is Multi-Factor Authentication?
 - Extends the usual username + password access by an additional factor
 - Avoids access to compromised accounts
 - Example: TAN as used for online banking

Using the cluster with Multi-Factor Authentication (Step by Step)

1. Login to RegApp
2. Add Token to Account
3. Upload a public SSH key (optional)
4. Assign SSH Key to Service HPC (optional)
5. Log In to a MFA Node

1. Login to RegApp

- Navigate to the RegApp
- Select your home organisation
- Log in using your SSO credentials



The screenshot shows the RegApp login interface. At the top left, there are logos for 'it RWTH AACHEN UNIVERSITY' and 'RWTH AACHEN UNIVERSITY'. At the top right, there are links for 'Site Credits', 'Privacy Policy', 'IT Center', and 'English'. Below the header is a blue bar with the text 'RegApp'. The main content area is titled 'Welcome' and contains the text: 'In order to use federated services you'll need a valid user account with one of the participating organizations. Please choose your home organization and click on "Proceed" or press enter.' Below this text are four input fields: 'Remember Home organisation:' with a checkbox, 'Federation:' with a dropdown menu set to 'All', 'Search filter:' with a text input field containing a vertical bar, and 'Home organization:' with a dropdown menu showing 'RWTH Aachen University'. At the bottom of the form is a blue button labeled 'PROCEED'.

1. Login to RegApp

RegApp

You have already registered with the following services:

RWTH High Performance Computing

The IT Center hosts one of the fastest supercomputers in Germany. The High Performance Computing group (HPC) supports users from all German universities including institutions from RWTH Aachen University in the efficient use of the central high-performance computing systems.

- [Service description](#)
- [Registry info](#)
- [Set service password](#)
- [Set SSH Key](#)

In order to see details of the services you registered with, click on the link 'Registry info' under the service.

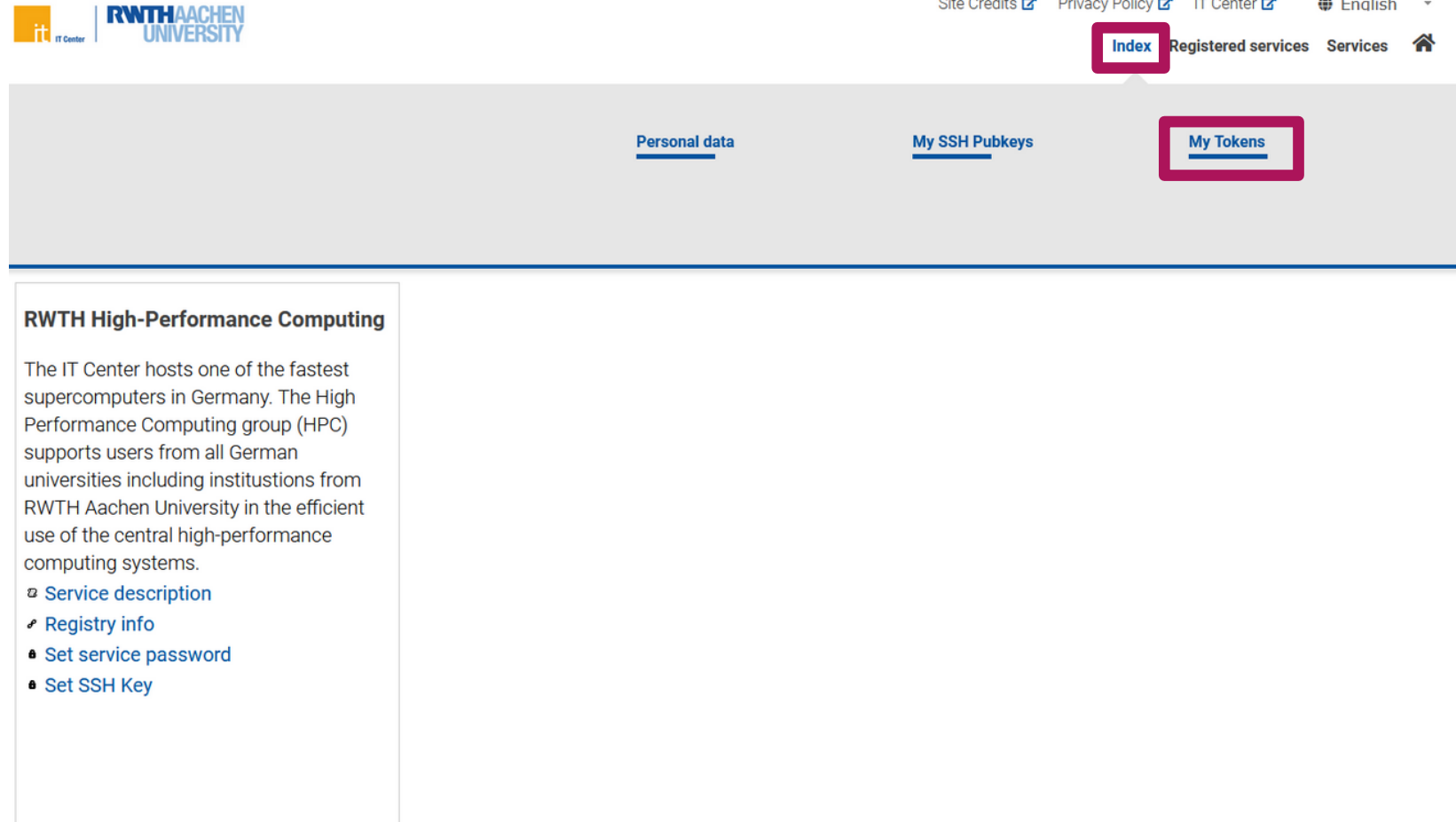
The following services are available:

To register with a service, click on the 'Register' link below the service, you want to register with.

- After login you see the RegApp dashboard
- Currently only one service configured (HPC)

2. Add Token to Account

- Only possible if you already have an HPC account
- Navigate to **Index** → **My Tokens**
(German: **Übersicht** → **Meine Tokens**)



The screenshot shows the HPC.NRW user interface. At the top left, there are logos for 'it Center' and 'RWTH AACHEN UNIVERSITY'. On the top right, there are links for 'Site Credits', 'Privacy Policy', 'IT Center', and a language selector set to 'English'. Below these, a navigation bar contains 'Index', 'Registered services', and 'Services'. The 'Index' link is highlighted with a red box. Below the navigation bar, there are three tabs: 'Personal data', 'My SSH Pubkeys', and 'My Tokens'. The 'My Tokens' tab is highlighted with a red box. Below the tabs, there is a section titled 'RWTH High-Performance Computing' with a description and a list of links: 'Service description', 'Registry info', 'Set service password', and 'Set SSH Key'.

In order to see details of the services you registered with, click on the link 'Registry info' under the service.

2. Add Token to Account

- Manage list of second factors (if your already have one)
- Add new tokens
 - **NEW SMARTPHONE TOKEN**
 - Recommended
 - Use an app like FreeOTP, Google Authenticator, Yubico Authenticator
 - Scan QR code
 - Confirm token
 - **CREATE NEW TAN LIST**
 - Backup only
 - Make list inaccessible for third parties

The screenshot shows the 'RegApp' interface for RWTH Aachen University. At the top, there are navigation links for Site Credits, Privacy Policy, IT Center, and English. Below the header, the 'List of second factors' section displays three entries:

Token icon	Token type	Active	Action
	Paper TAN list	Yes	DISABLE
	Smartphone app	Yes	DISABLE
	Smartphone app	Yes	DISABLE

Below the list, the 'Create a new token here.' section contains two buttons: 'NEW SMARTPHONE TOKEN' (highlighted with a red box) and 'CREATE NEW TAN LIST'. A 'Back' link is located at the bottom left.

The FreeOTP app screenshot shows a list of tokens for the user 'john.doe':

- bitbucket: 945 261
- reddit: 359 961
- reddit: 876 751
- Fedora: johndoe@redhat.com

A plus sign (+) is visible at the bottom right of the app interface.

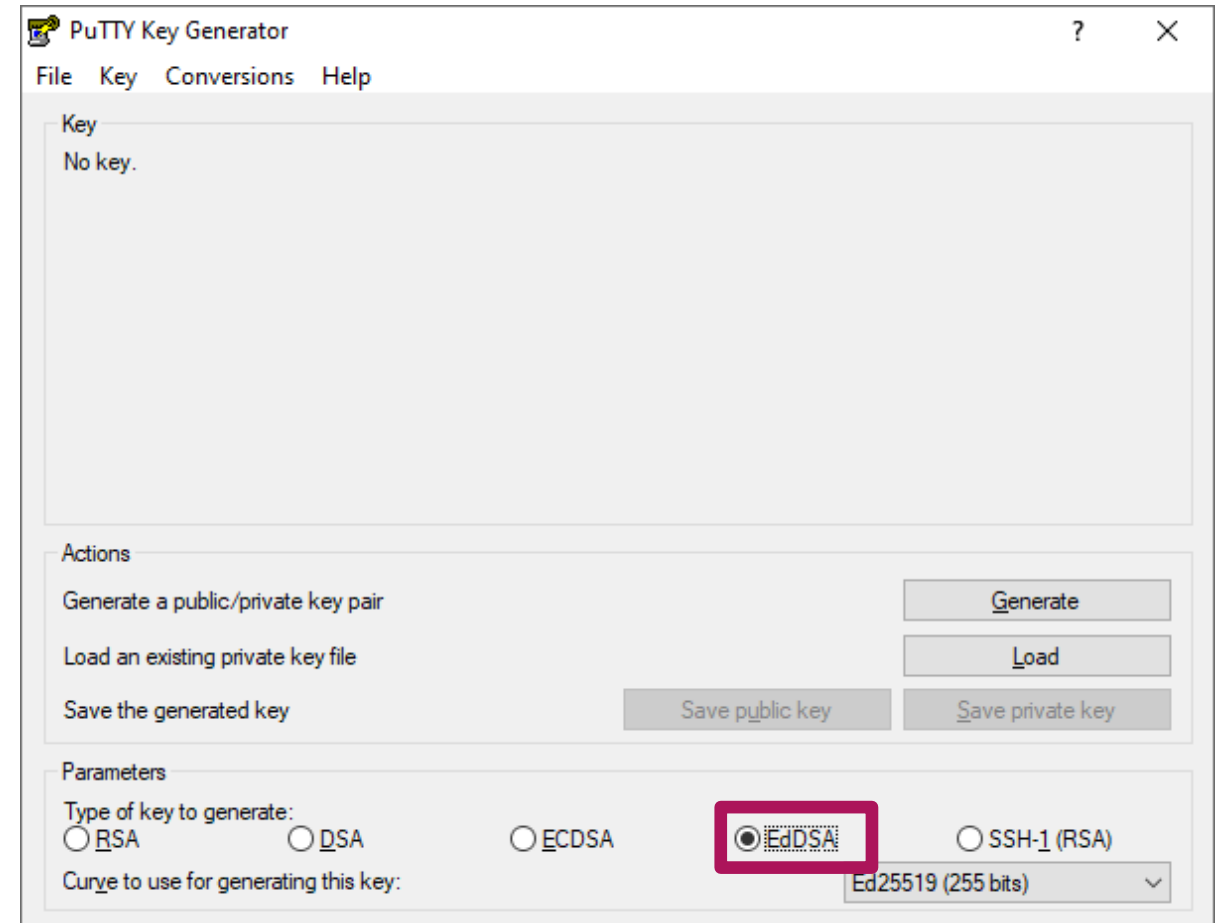
2. Add Token to Account

- Login using MFA now possible already (step 5)
- Disadvantage: You need the second factor for every login attempt now
- To avoid this: Use SSH key pairs associated with your account
- Then: Second factor only once every 10 hours required

3. Upload a public SSH key

- Generate a SSH Key Pair (if have not done before)
 - We recommend key type Ed25519
 - DON'T use keys without password
 - Use **strong** password for the private key
 - **NEVER** give away / upload your private key
 - Windows
 - You can use PuTTYgen <https://www.puttygen.com/>
 - Linux
 - You can use ssh-keygen

```
$ ssh-keygen -a 100 -t ed25519 \
-f ~/.ssh/id_ed25519
```



3. Upload a public SSH key





- In RegApp: Navigate to **Index** → **My SSH Pubkeys**



3. Upload a public SSH key

– Click **Add SSH Key**

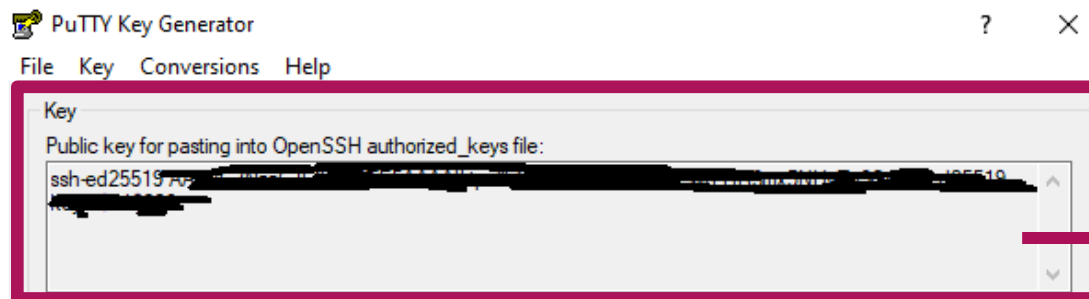
List of ssh keys

 HPC	 Work Laptop
Expires: 23.10.2022 14:48	Expires: 06.10.2022 10:01
Key type: ssh-rsa	Key type: ssh-rsa
Fingerprint (SHA256): OvKZI97PKrA5WoB3CnApBhzAEYG6NF IuvR2ZOrM3Gpk=	Fingerprint (SHA256): dnBFYrZwmUFB0ai2dxLNmyCPMHqGEh ubnG2261gTwCE=
Services: RWTH High-Performance Computing 	Services:
REVOKE	REVOKE
 Home Desktop	
Expires: 06.10.2022 10:02	
Key type: ssh-rsa	
Fingerprint (SHA256): aIDN9IKIYi/GziquNqOBIT /AEUVuHSDzM/bUYFj1Go=	
Services:	
REVOKE	

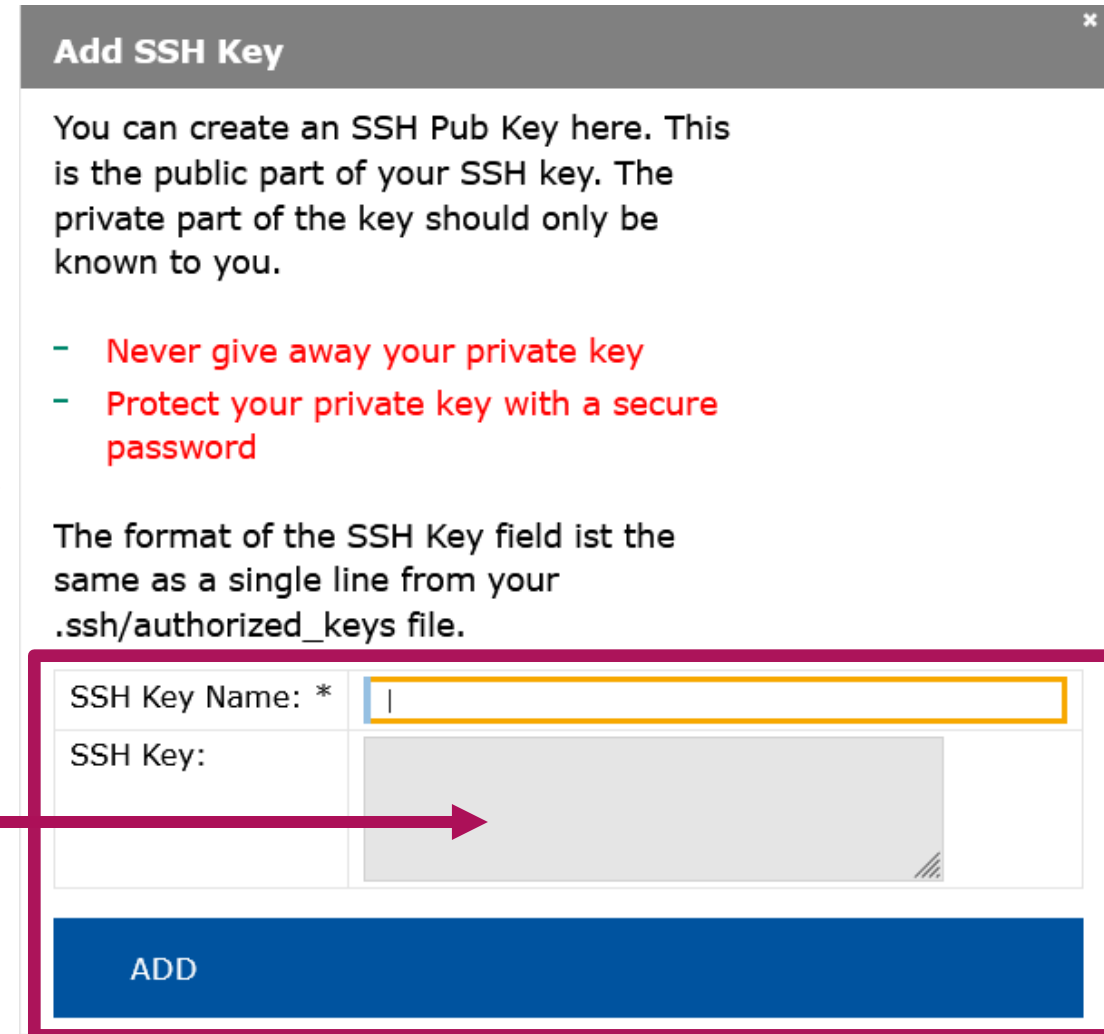
ADD SSH KEY

3. Upload a public SSH key

- Name the SSH Key
- Linux
 - Open public key (file ending „*.pub“)
 - Copy & paste key sequence to the text box
- Windows:
 - PuTTY uses different public key format
 - Open PuTTY Key Generator
 - Load key (if panel already closed)
 - Copy from “Public key for pasting into OpenSSH authorized_key file” & paste key sequence to the text box

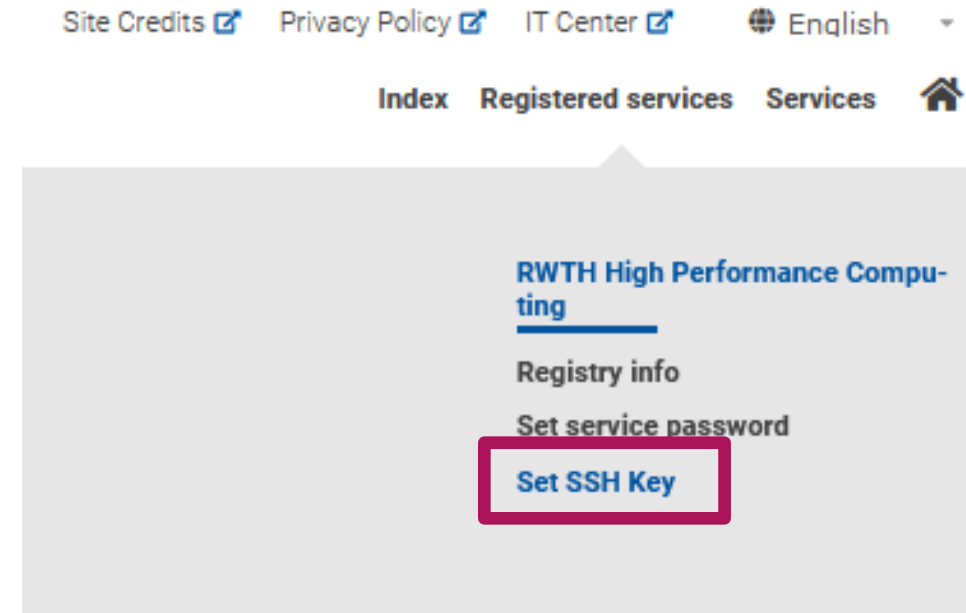


- Click **ADD**
- Do NOT upload your private key!



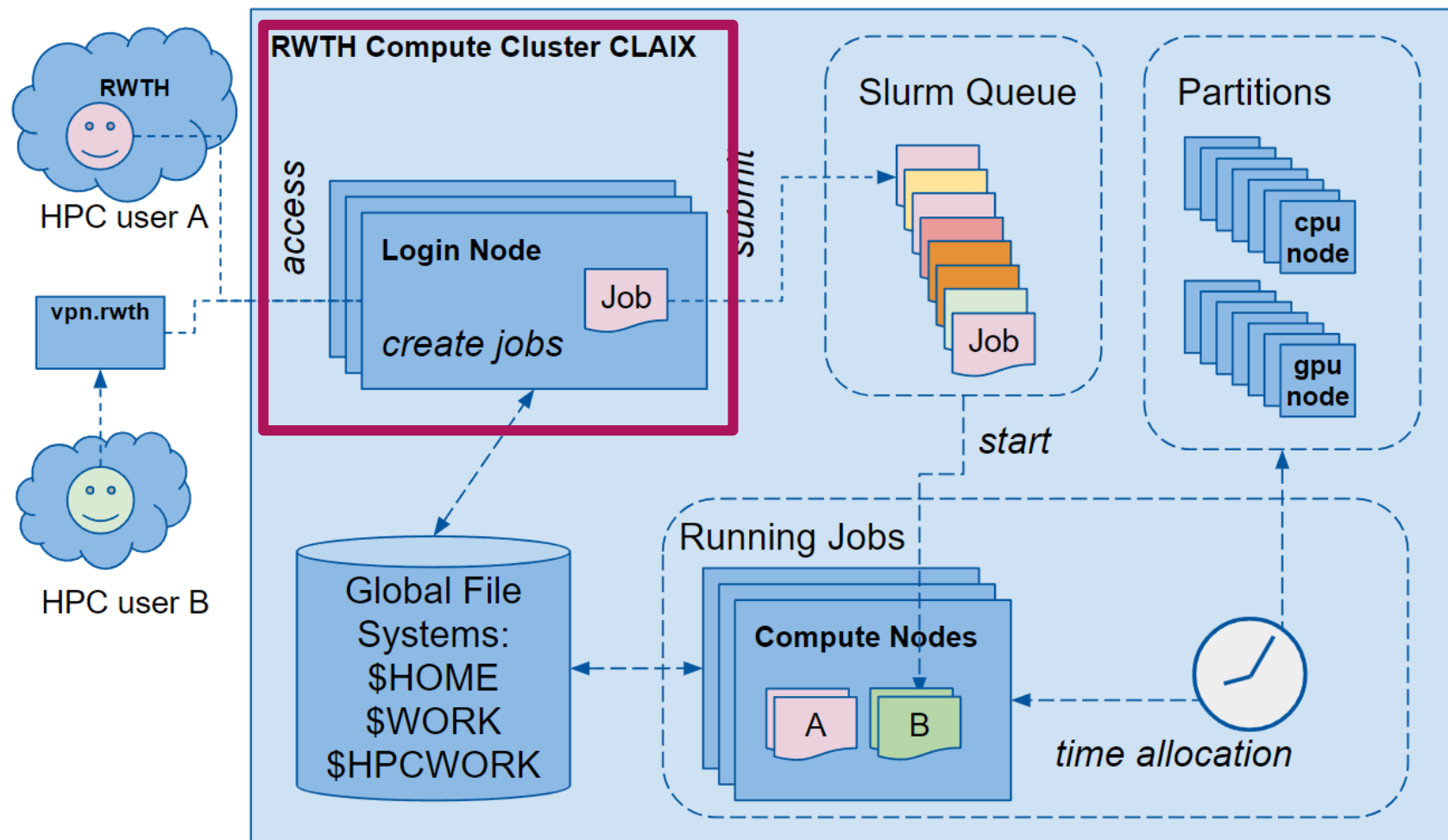
4. Assign SSH Key to Service HPC

- Navigate to **Registered Services** → **RWTH High Performance Computing** → **Set SSH Key**
- Click **Add** on the SSH key you wish to associate
- Fill in the required fields
- Click Add to associate the key with your HPC account
- Note: The SSH Key is set to automatically expire after a certain amount of time, no reuse possible



Login to CLAIX

CLAIX Usage - Overview



5. Log In to a MFA Node

- Connect to the RWTH VPN / use “trusted” network
- Login per native ssh, PuTTY, WSL or FastX possible
- Use one of the dialog nodes, e.g.:
 - `login23-1.hpc.itc.rwth-aachen.de`
 - `login23-2.hpc.itc.rwth-aachen.de`
 - `login23-3.hpc.itc.rwth-aachen.de`
 - `login23-4.hpc.itc.rwth-aachen.de`
- Different frontends for different purposes:
 - X-Session:** `login23-x-{1,2}.hpc.itc.rwth-aachen.de`
 - File transfers:** `copy23-{1,2}.hpc.itc.rwth-aachen.de`
 - GPU system:** `login23-g-{1,2}.hpc.itc.rwth-aachen.de`
- You will be asked for username, password and second factor

5. Log In to a MFA Node

Example 1: ssh via commandline

```
name@local: $
```


5. Log In to a MFA Node

Example 1: ssh via commandline

```
name@local: $ ssh -l ab12345 login23-1.hpc.itc.rwth-aachen.de
```

5. Log In to a MFA Node

Example 1: ssh via commandline

```
name@local: $ ssh -l ab12345 login23-1.hpc.itc.rwth-aachen.de
The authenticity of host 'login23-1.hpc.itc.rwth-aachen.de (134.61.44.117)' can't be established.
ECDSA key fingerprint is SHA256:Q80xbVMJcF1Nnb4WtP9/rzt3FOcU52iLbmGOMtxcfDg.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

5. Log In to a MFA Node

Example 1: ssh via commandline

```
name@local: $ ssh -l ab12345 login23-1.hpc.itc.rwth-aachen.de
The authenticity of host 'login23-1.hpc.itc.rwth-aachen.de (134.61.44.117)' can't be established.
ECDSA key fingerprint is SHA256:Q80xbVMJcF1Nnb4WtP9/rzt3FOcU52iLbmGOMtxcfDg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? Yes
```

5. Log In to a MFA Node

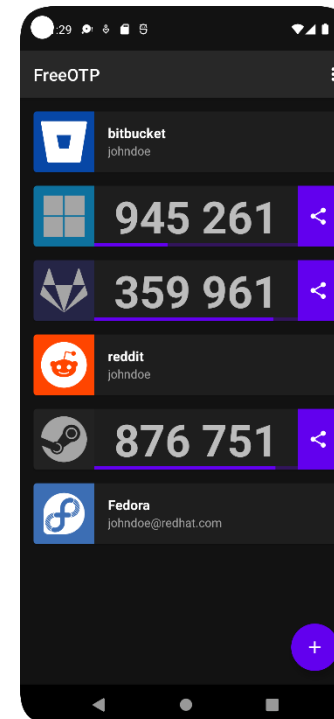
Example 1: ssh via commandline

```
name@local: $ ssh -l ab12345 login23-1.hpc.itc.rwth-aachen.de
The authenticity of host 'login23-1.hpc.itc.rwth-aachen.de (134.61.44.117)' can't be established.
ECDSA key fingerprint is SHA256:Q80xbVMJcF1Nnb4WtP9/rzt3FOcU52iLbmGOMtxcfDg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? Yes
Warning: Permanently added 'login23-1.hpc.itc.rwth-aachen.de, 134.61.44.117' (ECDSA) to the list of known hosts.
Password:
```

5. Log In to a MFA Node

Example 1: ssh via commandline

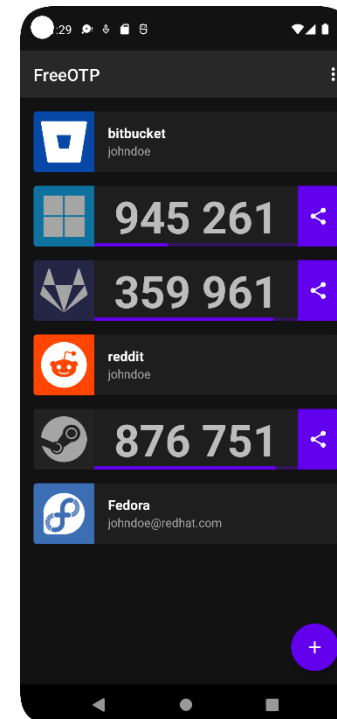
```
name@local: $ ssh -l ab12345 login23-1.hpc.itc.rwth-aachen.de
The authenticity of host 'login23-1.hpc.itc.rwth-aachen.de (134.61.44.117)' can't be established.
ECDSA key fingerprint is SHA256:Q80xbVMJcF1Nnb4WtP9/rzt3FOcU52iLbmGOMtxcfDg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? Yes
Warning: Permanently added 'login23-1.hpc.itc.rwth-aachen.de, 134.61.44.117' (ECDSA) to the list of known hosts.
Password: *****
Two-factor code:
```



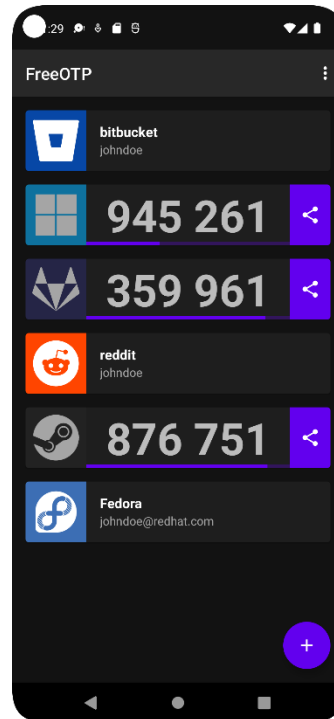
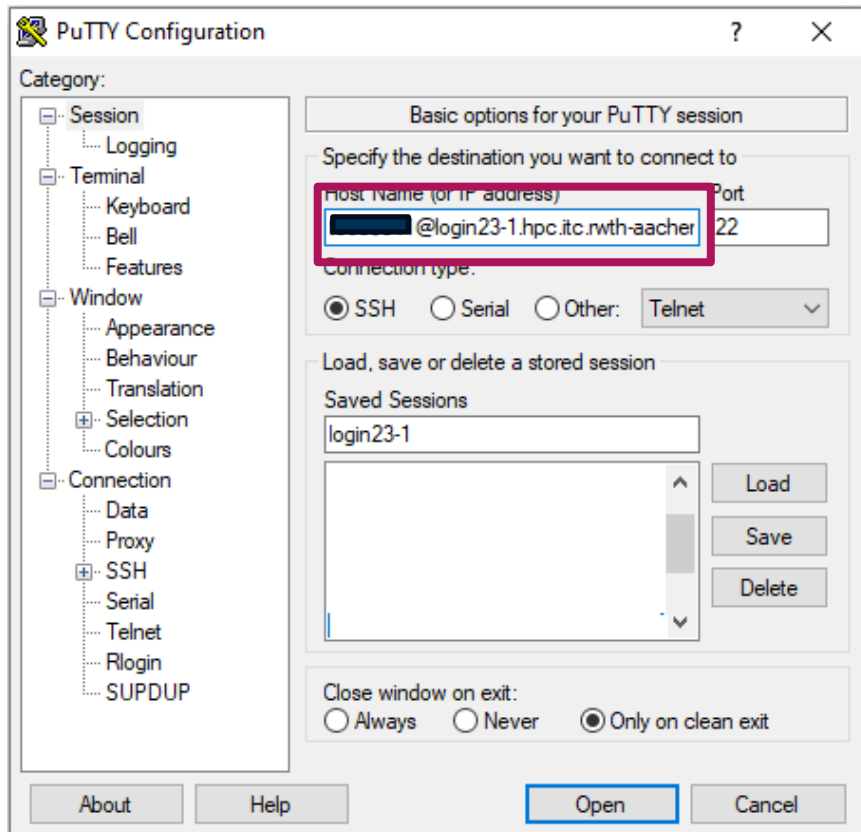
5. Log In to a MFA Node

Example 1: ssh via commandline

```
name@local: $ ssh -l ab12345 login23-1.hpc.itc.rwth-aachen.de
The authenticity of host 'login23-1.hpc.itc.rwth-aachen.de (134.61.44.117)' can't be established.
ECDSA key fingerprint is SHA256:Q80xbVMJcF1Nnb4WtP9/rzt3FOcU52iLbmGOMtxcfDg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? Yes
Warning: Permanently added 'login23-1.hpc.itc.rwth-aachen.de, 134.61.44.117' (ECDSA) to the list of known hosts.
Password: *****
Two-factor code: *****
```

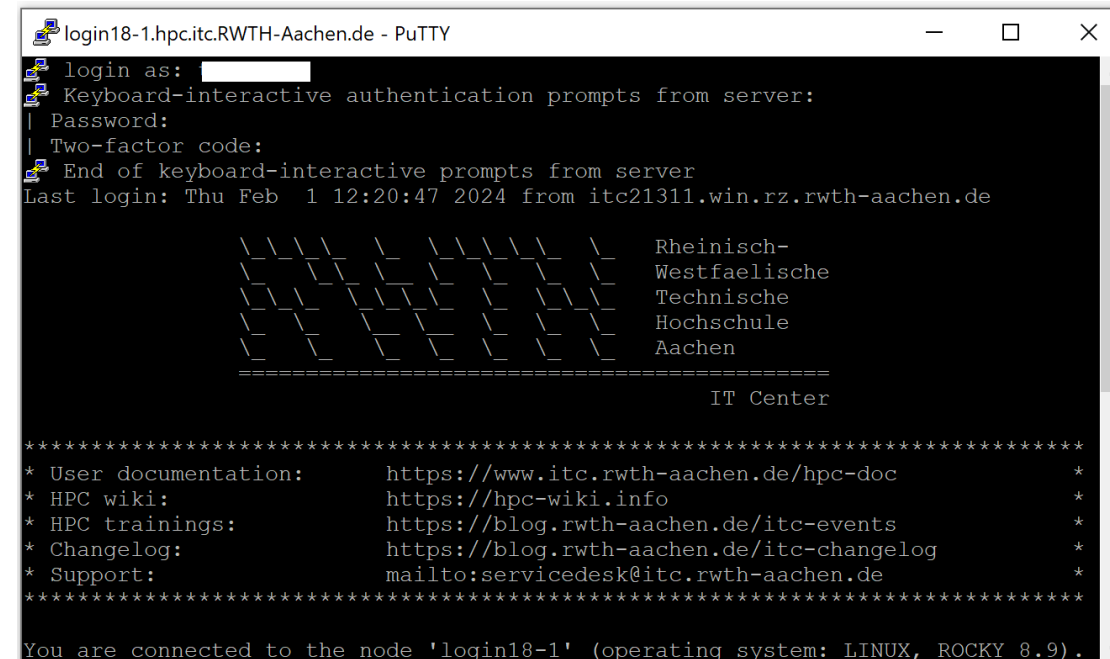


5. Log In to a MFA Node



Example 2: PuTTY

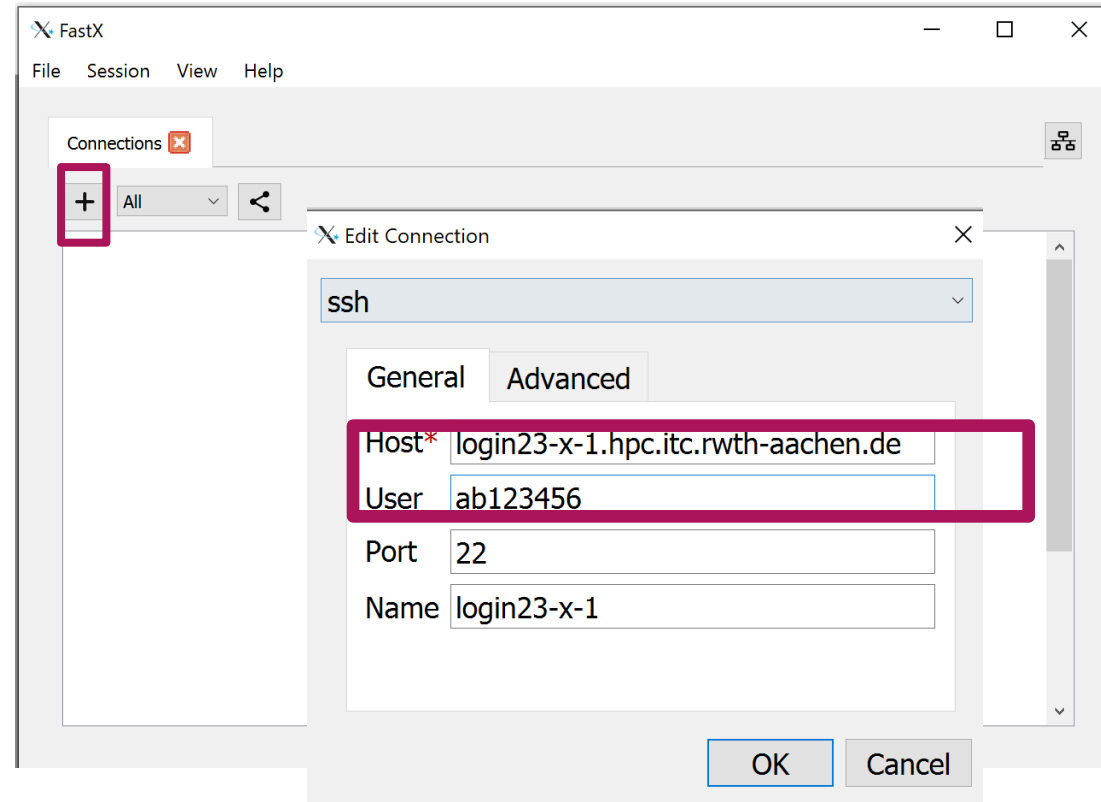
1. Open “PuTTY”.
2. Specify a host name, e.g. “login23-1.hpc.itc.rwth-aachen.de”
3. If you want, you can add a session name and “Save” this session.
4. “Open” the connection.
5. Denote your HPC account and afterwards state your password.
6. Enter your two-factor code.
7. You may have to confirm that the host is a trusted machine



5. Log In to a MFA Node

Example 3: FastX

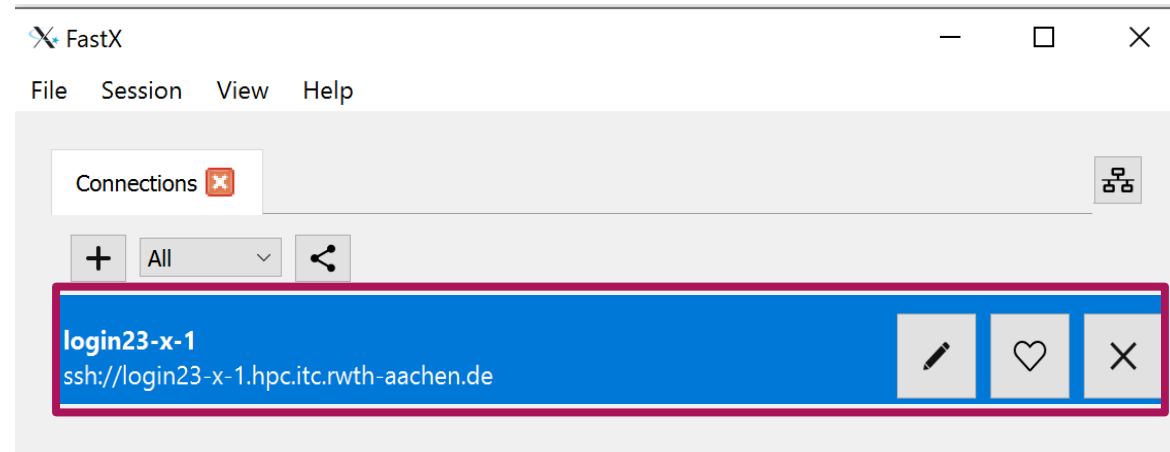
1. Download here <https://www.starnet.com/download/fastx-client>
2. Open client
3. Click +
4. Select “ssh”
5. Use e.g. login23-x-1.hpc.itc.rwth-aachen.de as host



5. Log In to a MFA Node

Example 3: FastX

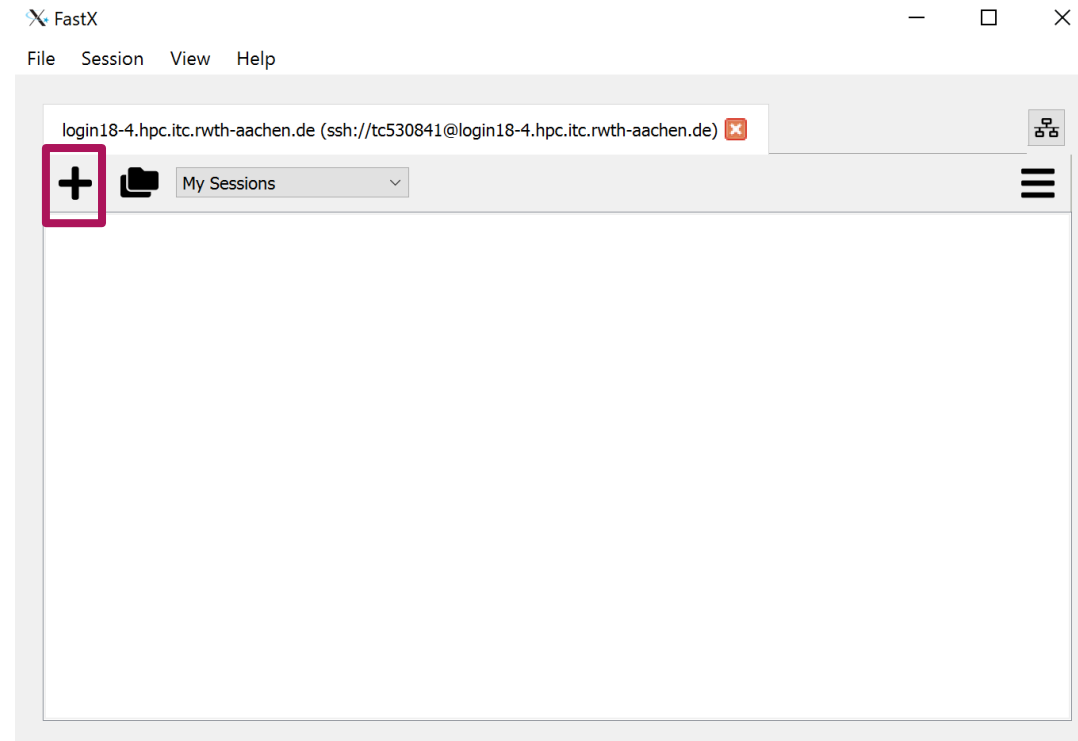
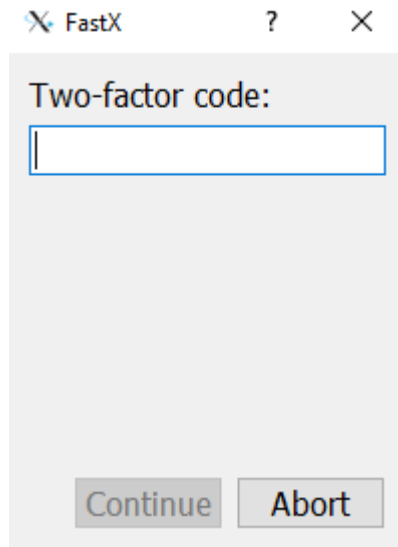
1. Download here <https://www.starnet.com/download/fastx-client>
2. Open client
3. Click +
4. Select “ssh”
5. Use e.g. login23-x-1.hpc.itc.rwth-aachen.de as host
6. Double click on new connection



5. Log In to a MFA Node

Example 3: FastX

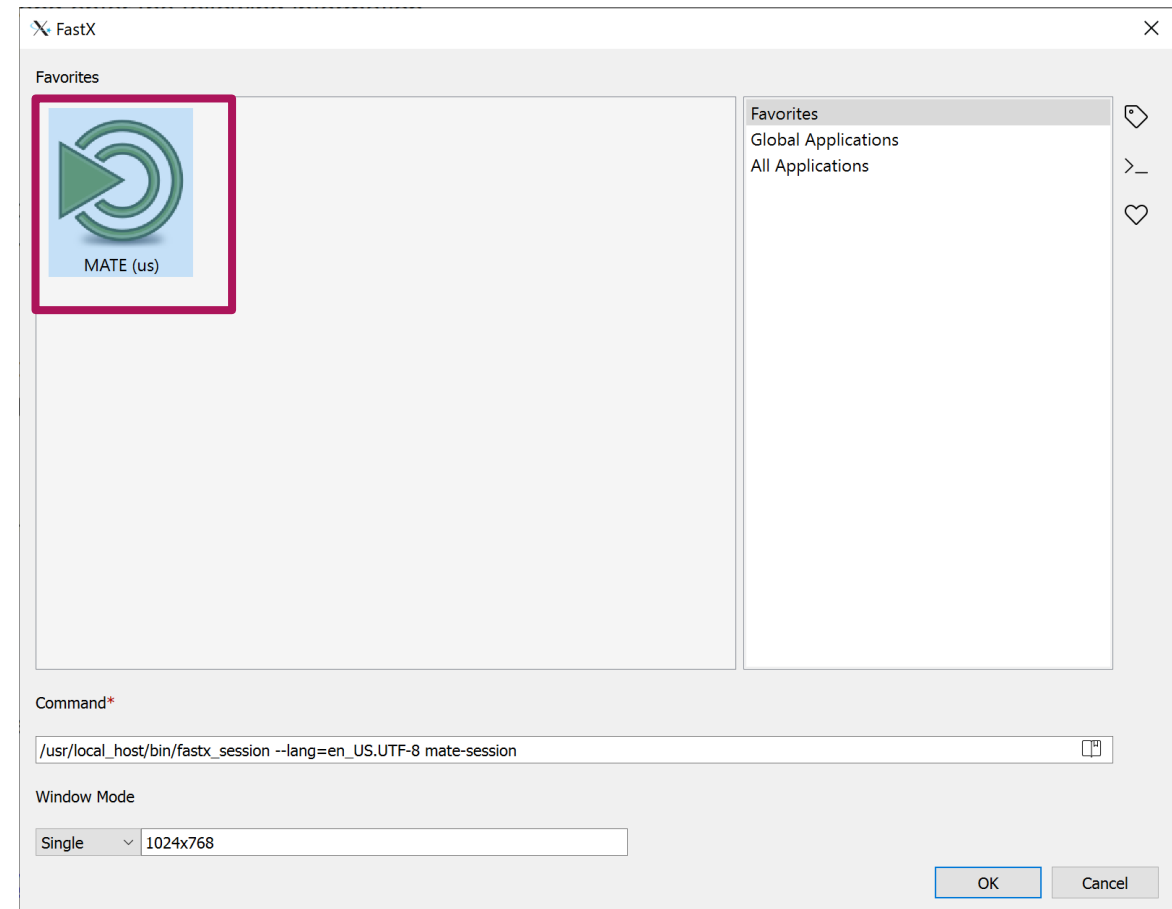
1. Download here <https://www.starnet.com/download/fastx-client>
2. Open client
3. Click +
4. Select “ssh”
5. Use e.g. `login23-x-1.hpc.itc.rwth-aachen.de`
6. Double click on new connection
7. Click +
8. Type user name
9. Type password
10. Type two-factor code



5. Log In to a MFA Node

Example 3: FastX

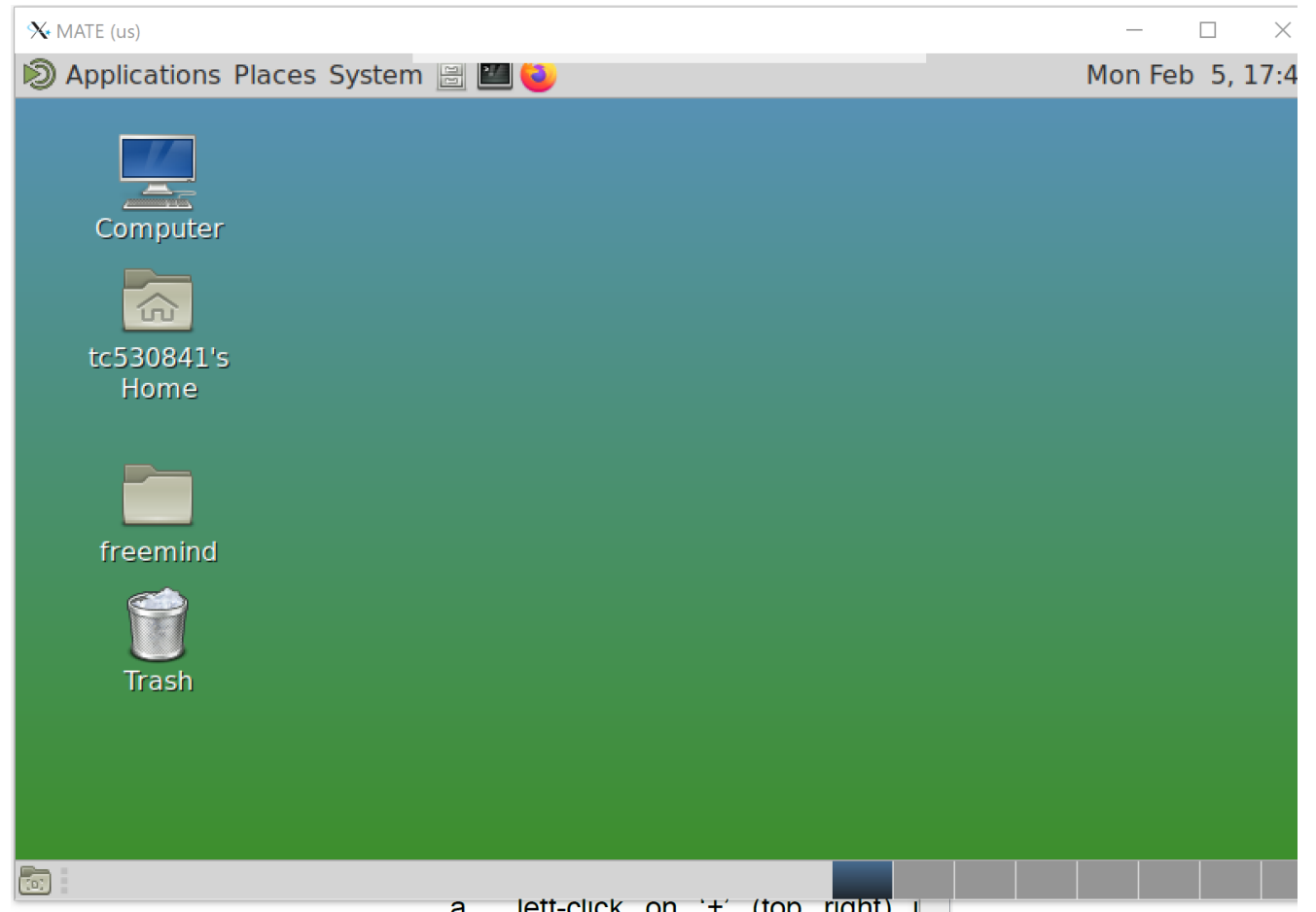
1. Download here <https://www.starnet.com/download/fastx-client>
2. Open client
3. Click +
4. Select “ssh”
5. Use e.g. `login23-x-1.hpc.itc.rwth-aachen.de`
6. Double click on new connection
7. Click +
8. Type user name
9. Type password
10. Type two-factor code
11. Select an environment (e.g., MATE)



5. Log In to a MFA Node

Example 3: FastX

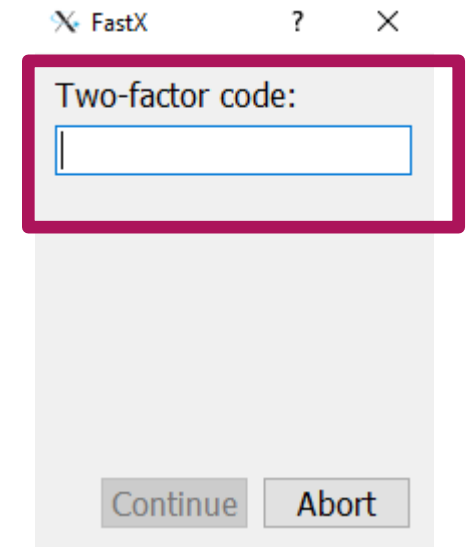
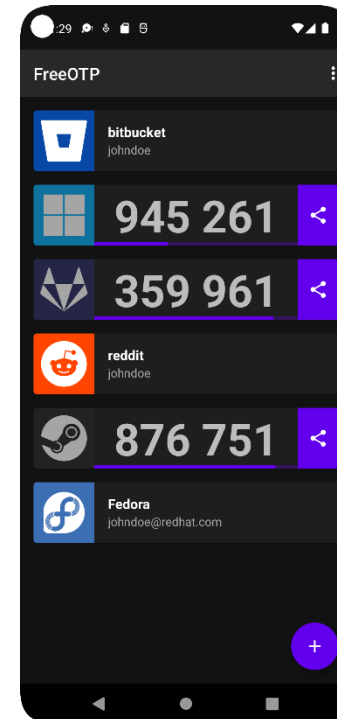
1. Download here <https://www.starnet.com/download/fastx-client>
2. Open client
3. Click +
4. Select “ssh”
5. Use e.g. `login23-x-1.hpc.itc.rwth-aachen.de`
6. Double click on new connection
7. Click +
8. Type user name
9. Type password
10. Type two-factor code
11. Select an environment (e.g., MATE)
12. Use full graphical remote session



5. Log In to a MFA Node

Up to now:

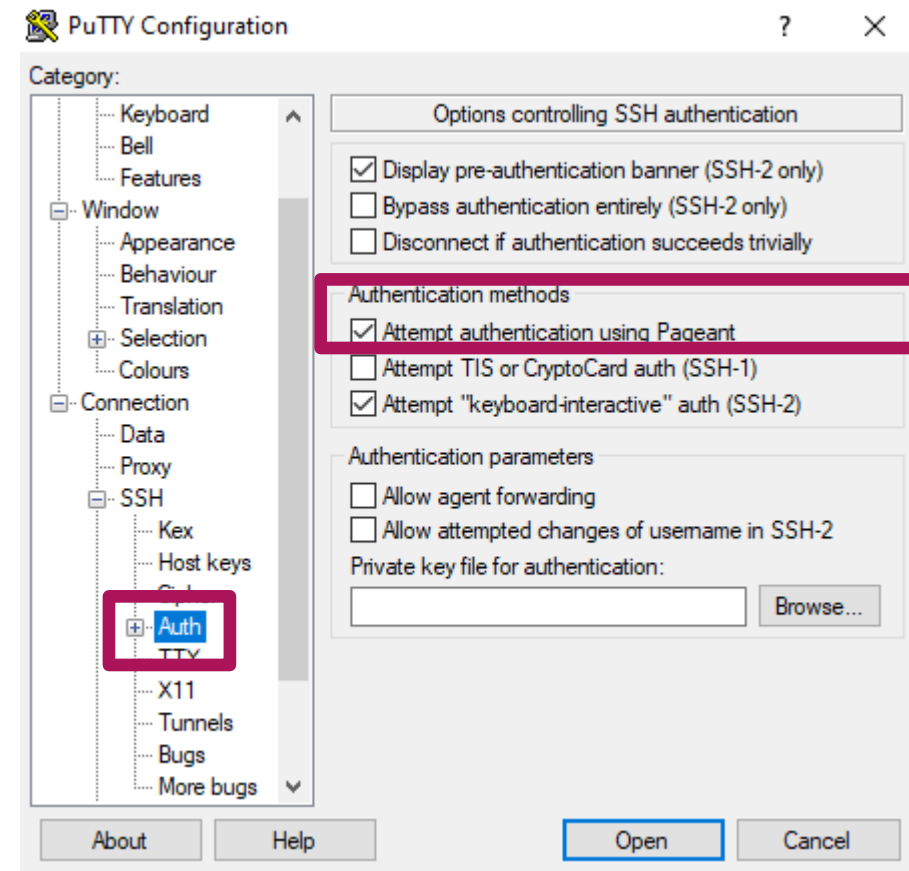
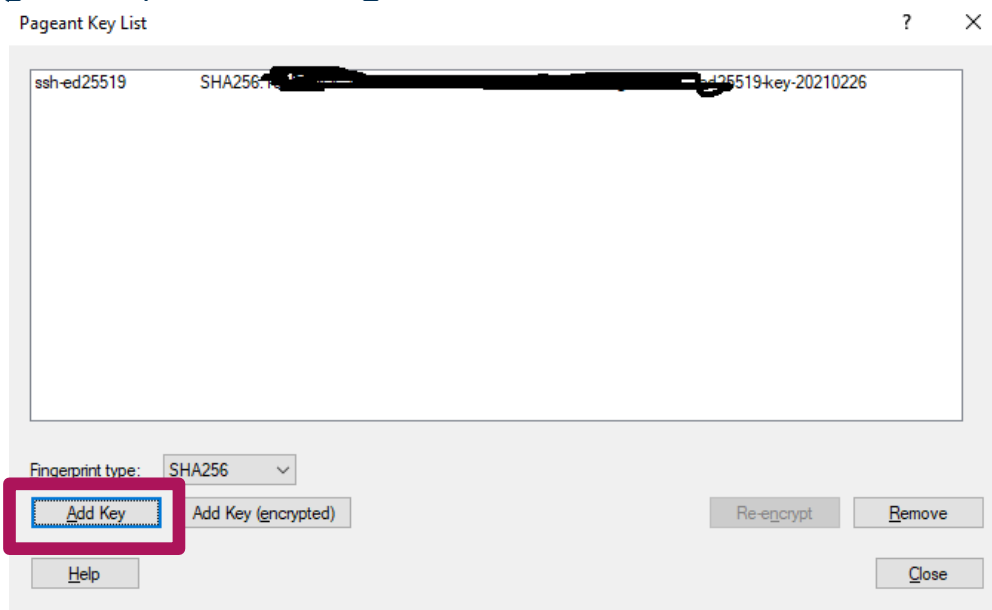
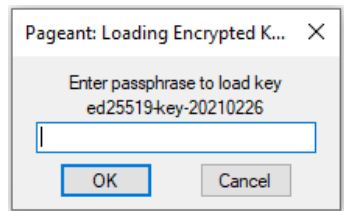
Second factor only once within 10 hours,
if you use an ssh key



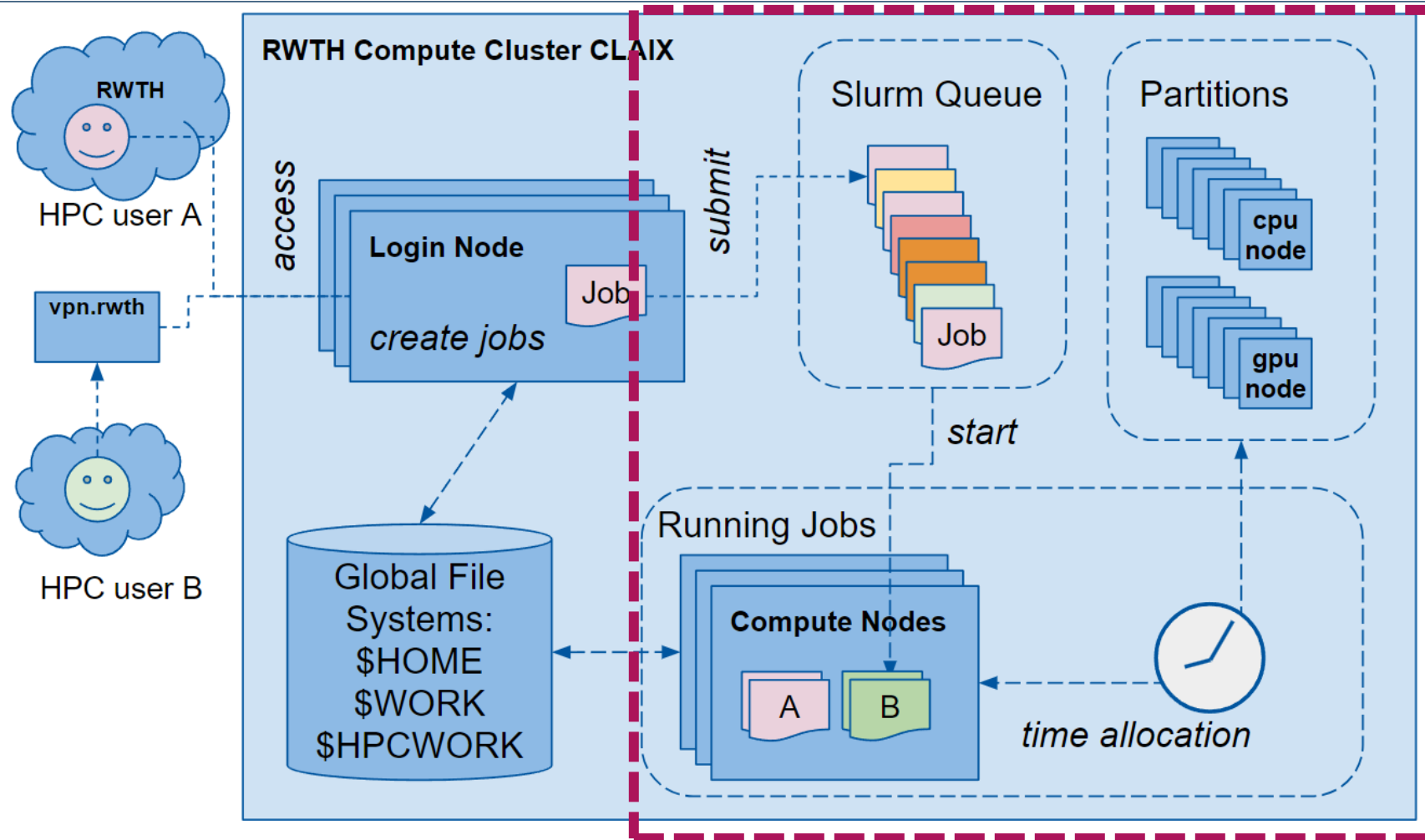
5. Log In to a MFA Node

- Key agents might support you
 - Linux

```
$ eval `ssh-agent`  
$ ssh-add ~/.ssh/id_ed25519
```
 - Windows
 - Use PuTTY Pageant (also for login via FastX, WinSCP, etc.)



CLAIX Usage - Overview



Usage of Slurm
→ Talk by Alvaro

- MFA helps to secure your personal and research data
- Smart Phone App preferred, use TAN list as backup!
- In case of problems
 - Use the consultation hours:
<https://blog.rwth-aachen.de/itc-events/en/events/kategorie/wiederkehrend/hpc-consultation-hour>
 - Contact servicedesk@itc.rwth-aachen.de

Questions?