

TECHNISCHE
UNIVERSITÄT
DARMSTADT

RWTHAACHEN
UNIVERSITY

Using multi-factor authentication for CLAIX

Tim Cramer

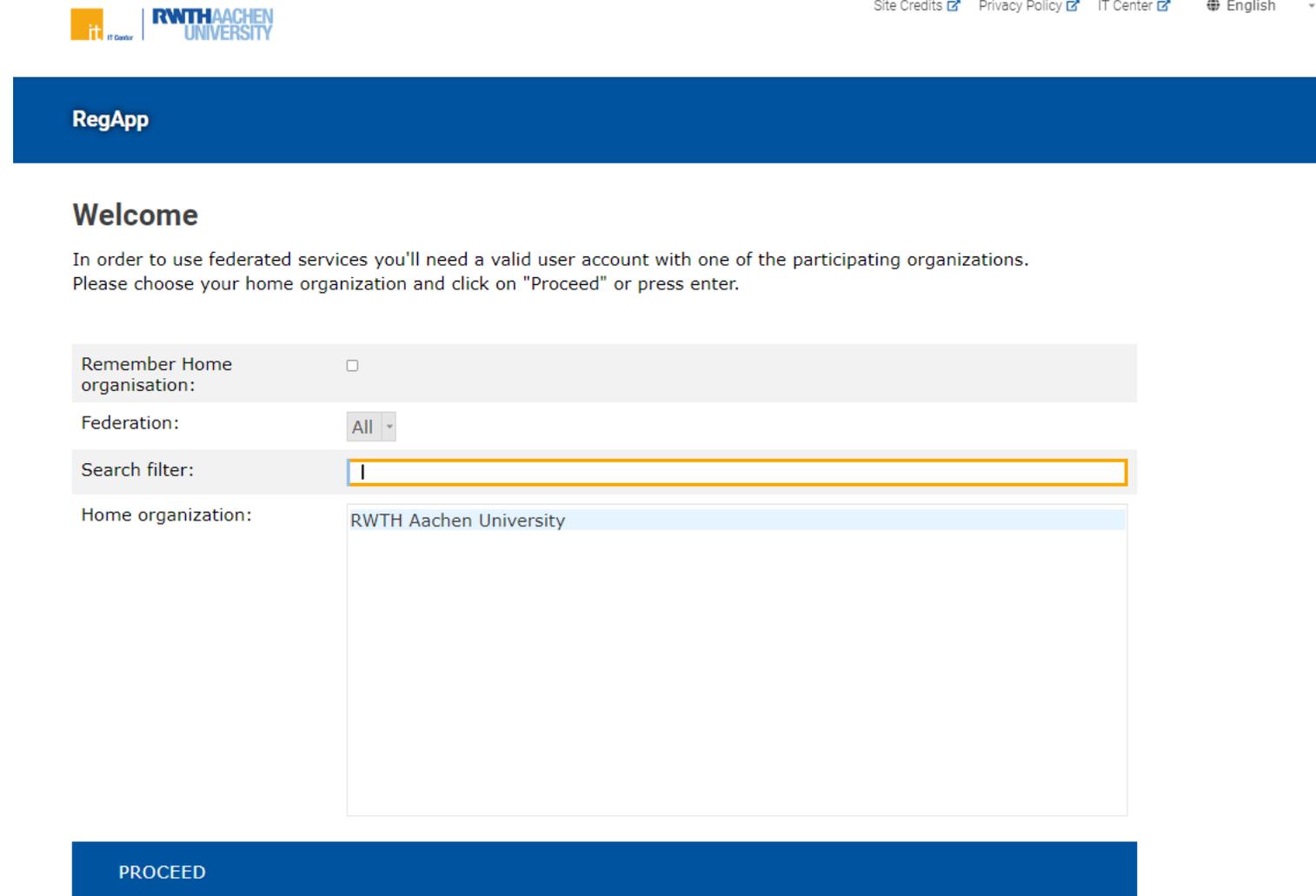
- What is RegApp?
 - Selfservice portal for HPC accounts
 - Register for the service
 - Change your HPC account password
 - Upload and manage SSH keys
 - Registering tokens for multi-factor authentication (**mandatory after January, 15th 2024**)
 - <https://regapp.itc.rwth-aachen.de/>
- What is Multi-Factor 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 IT Center' 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 dark blue bar with the text 'RegApp'. The main content area has a 'Welcome' heading and a paragraph: '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 is a form with the following 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 list box containing 'RWTH Aachen University'. At the bottom of the form is a large 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.

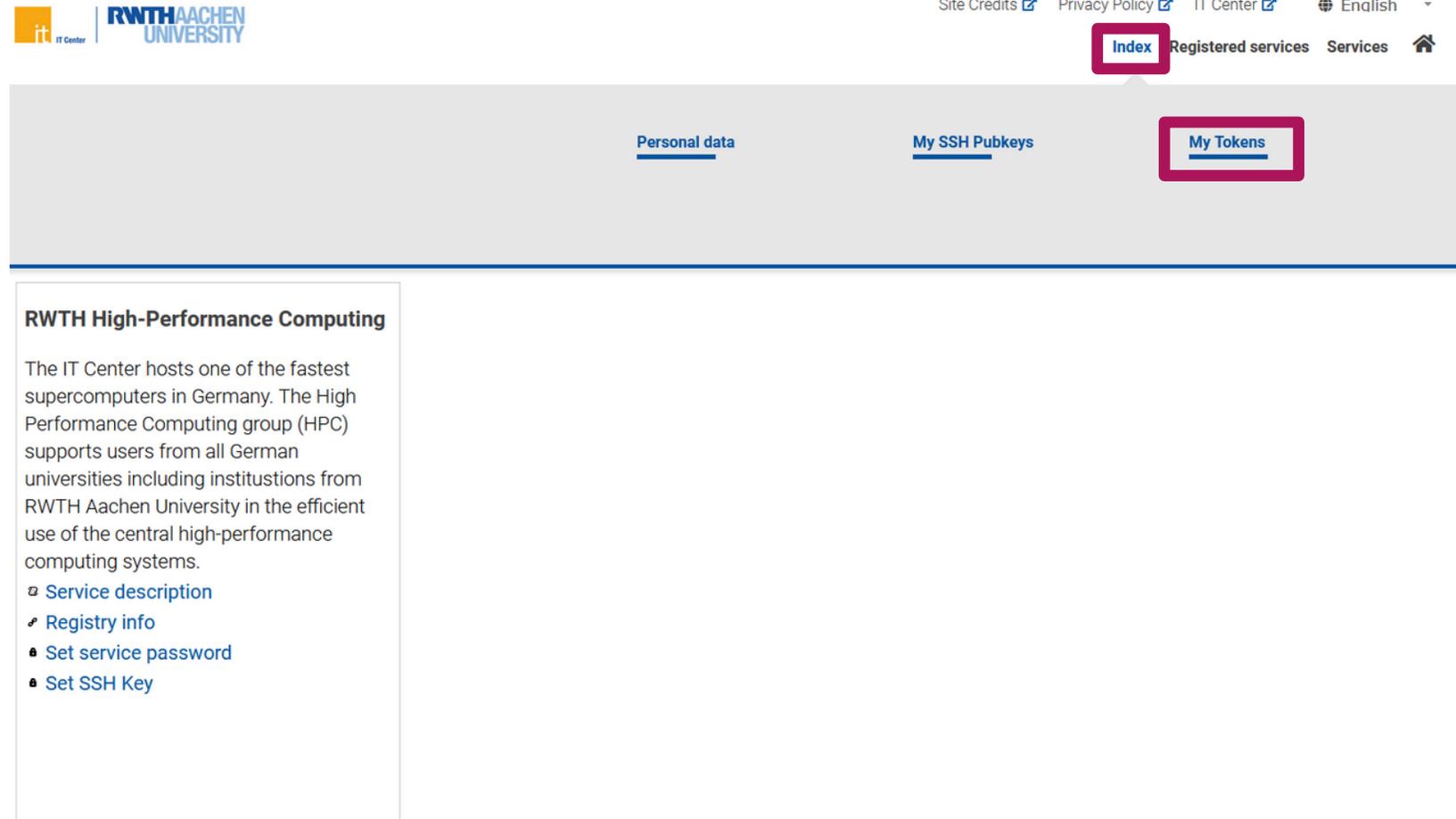
The following services are available:

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 IT Center' and 'RWTH AACHEN UNIVERSITY'. On the top right, there are links for 'Site Credits', 'Privacy Policy', 'IT Center', and 'English'. Below these, there is a navigation bar with 'Index' (highlighted with a red box), 'Registered services', and 'Services'. Underneath, there is a secondary navigation bar with 'Personal data', 'My SSH Pubkeys', and 'My Tokens' (highlighted with a red box). The main content area features 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

RegApp

List of second factors

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

Create a new token here.

- NEW SMARTPHONE TOKEN
- CREATE NEW TAN LIST

Back

FreeOTP

- bitbucket john.doe
- 945 261
- 359 961
- reddit john.doe
- 876 751
- Fedora john.doe@redhat.com

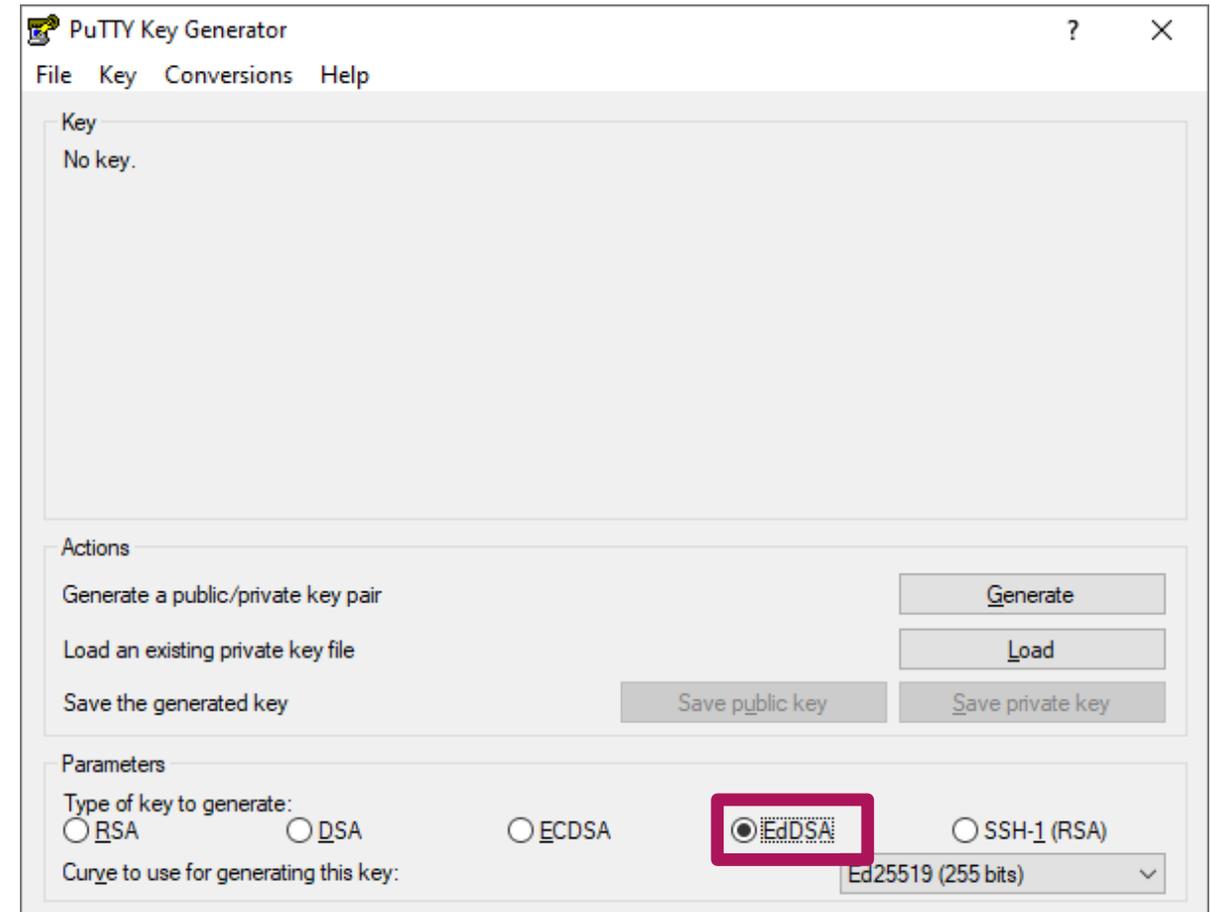
2. Add Token to Account

- 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**

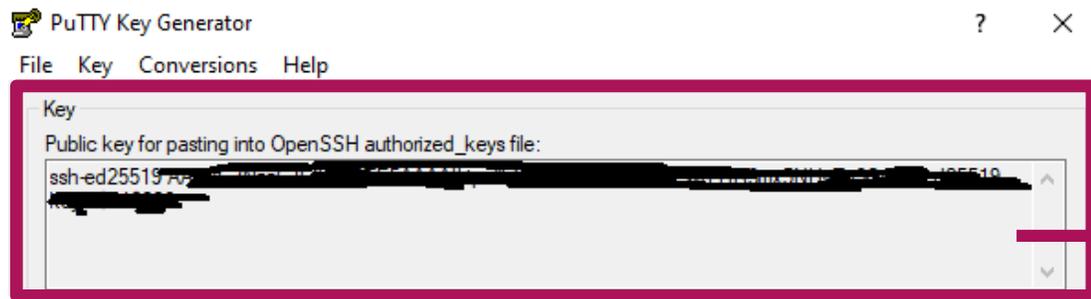
List of ssh keys

 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/GzqiqhNqOBIT /AEUVuHSDzM/bUYFjJ1Go=	
Services:	
REVOKE	

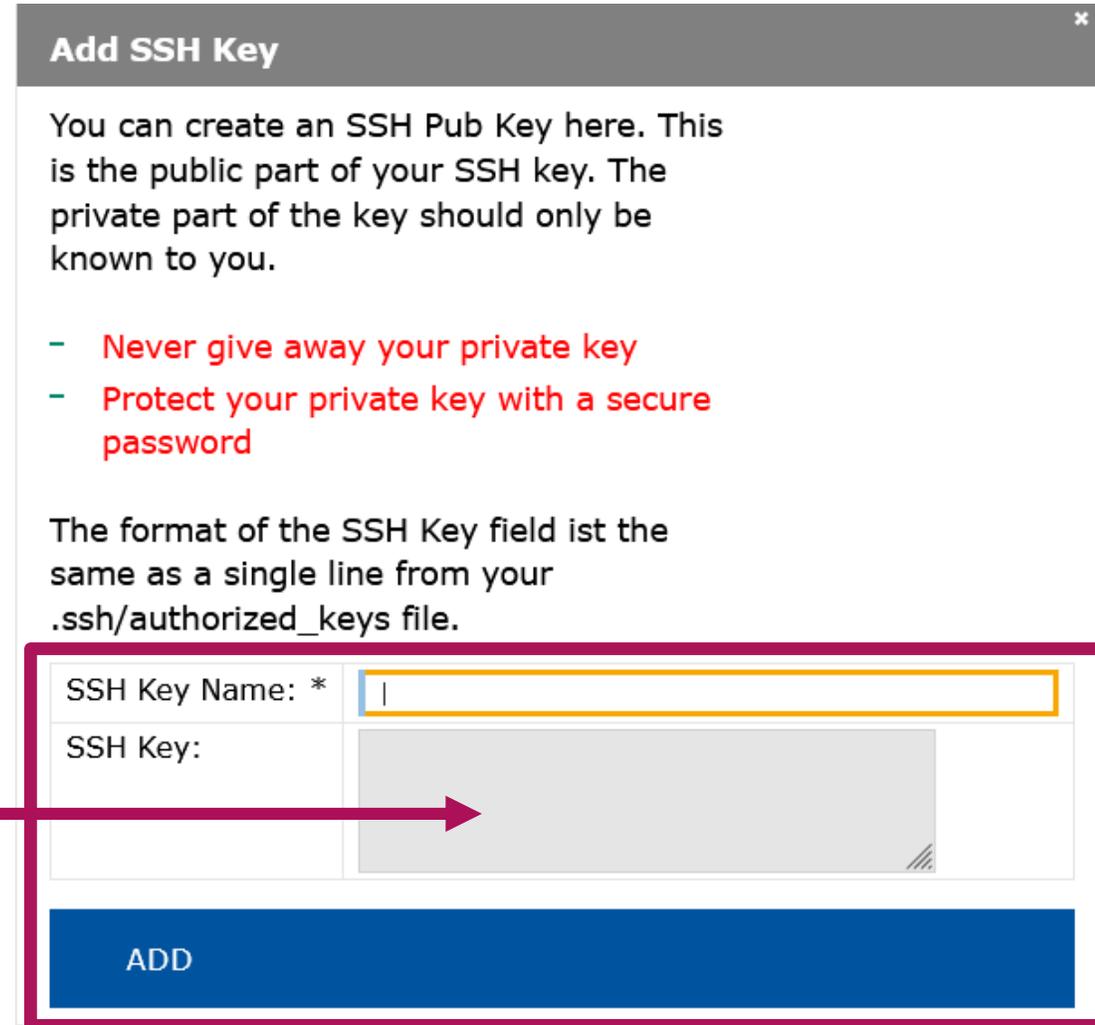
ADD SSH KEY

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

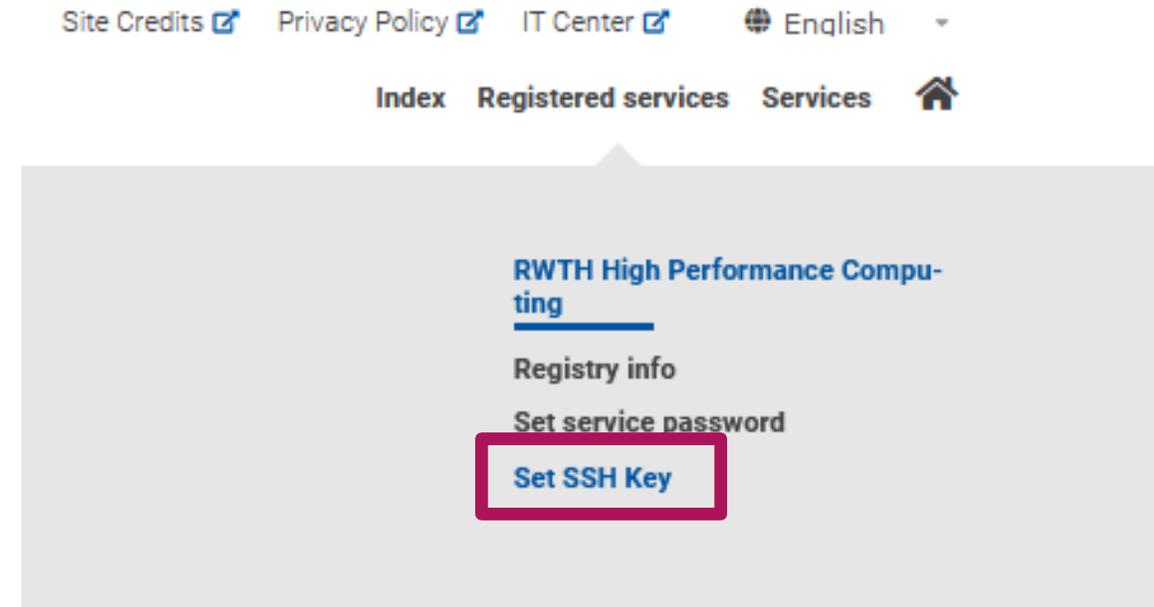


- Click **ADD**
- Do NOT upload your private key!



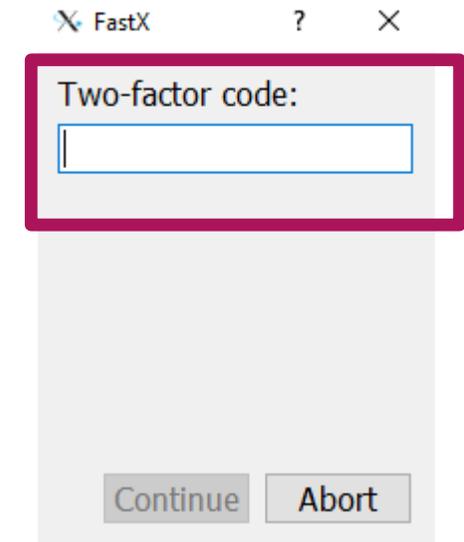
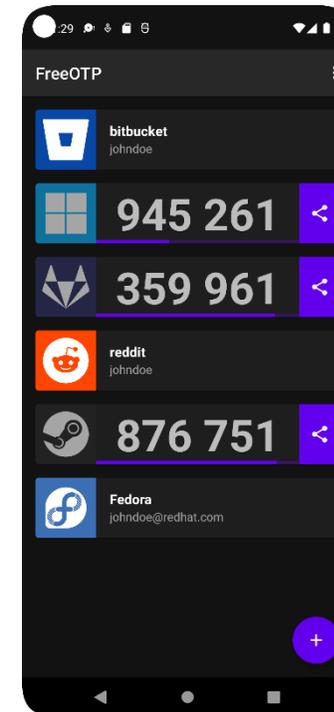
4. Assign SSH Key to Service HPC

- 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



5. Log In to a MFA Node

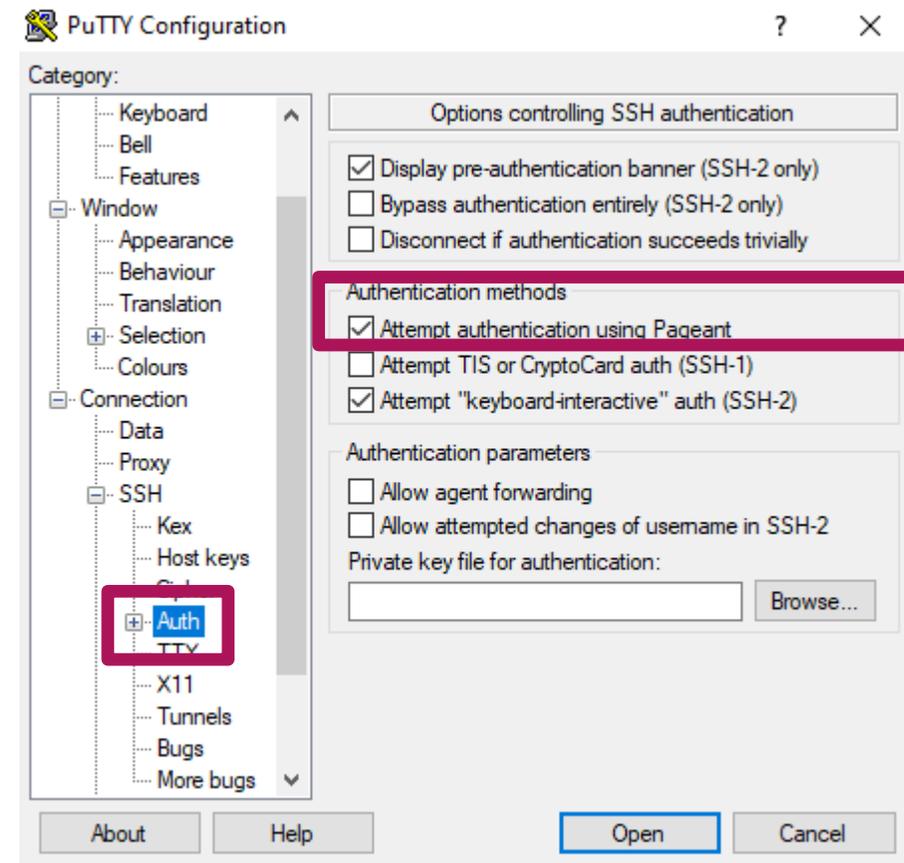
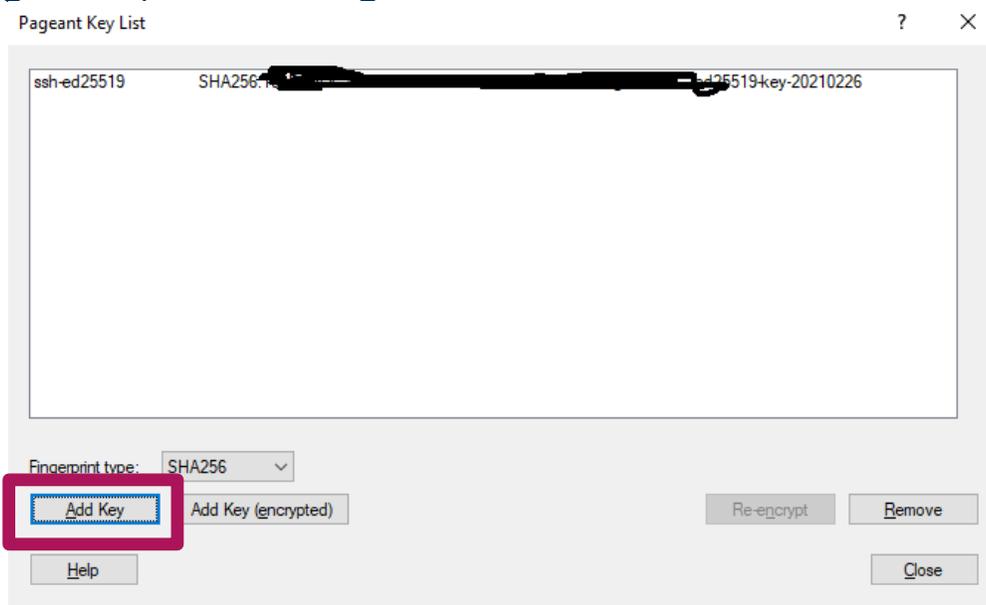
- Use one of the dialog nodes, e.g.:
`login18-1.hpc.itc.rwth-aachen.de`
`login18-2.hpc.itc.rwth-aachen.de`
`login18-3.hpc.itc.rwth-aachen.de`
`login18-4.hpc.itc.rwth-aachen.de`
- Login per ssh, PuTTY or FastX possible
- You will be asked for username, password and second factor
- Second factor only once 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.)



- MFA helps to secure your personal and research data
- Workflows might change a bit
- MFA is mandatory for the HPC system after January 15th, 2024
- 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?