Agenda

Part I

basic information about HPC **resources**

Monday

13:30 - 13:35	Welcome Day 1	Tim Cramer
13:35 - 14:05	HPC Architecture Basics and RWTH Resources	Tim Cramer
14:05 - 14:35	Storage Strategy for HPC Users	Philipp Martin
14:35 - 14:40	Break	
14:40 - 15:25	NHR and RWTH Computing Projects	Tim Cramer
15:25 - 16:00	Introduction to JupyterHub	Alvaro Frank

Part II

basic information about HPC **usage**

Tuesday

09:00 - 09:05	Welcome Day 2	Tim Cramer
09:05 - 09:35	Access to CLAIX and Using multi-factor Authentication	Tim Cramer
09:35 - 10:05	Cluster Software Environment HPC	Felix Tomski
10:05 – 10:45	Introduction to Slurm	Alvaro Frank
10:45 - 11:00	Break	
11:00 - 11:45	Parallel Programming Overview	Tim Cramer
11:45 - 12:30	Performance Metrics & Measurements	Felix Tomski
12:30 - 12:45	Closing Session	Tim Cramer

HPC.NRW

NHR4CES NHR for Computational Engineering Science

TECHNISCHE UNIVERSITÄT DARMSTADT

RWTH AACHEN UNIVERSITY

Access to CLAIX and Using multi-factor Authentication

Tim Cramer

GREAT COMPUTING COMES WITH GREAT SUPPORT.

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

Exception: RWTH projects for members of FZJ

- 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

Access

- 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/rhr4fjjutttf/article/598d0f7f78cb4ab8b81af1b3f68ba831

VPN

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

IDM Account

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

Multi-Factor Authentication

- 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

HPC Account

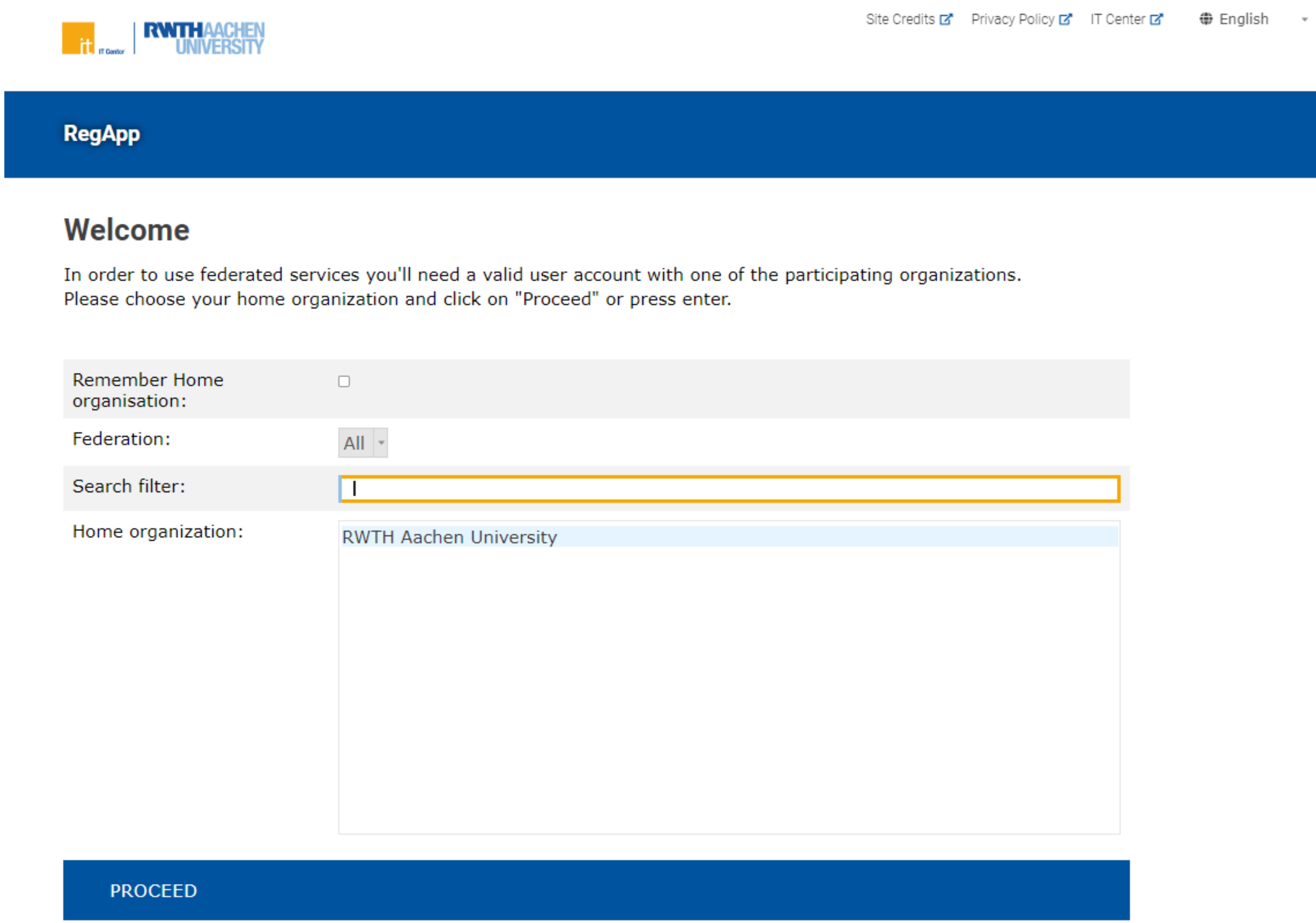
- What is Multi-Factor Authentication?
  - Extends the usual username + password access by an additional factor
  - Avoids access to compromised accounts
  - Example: TAN as used for online banking

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



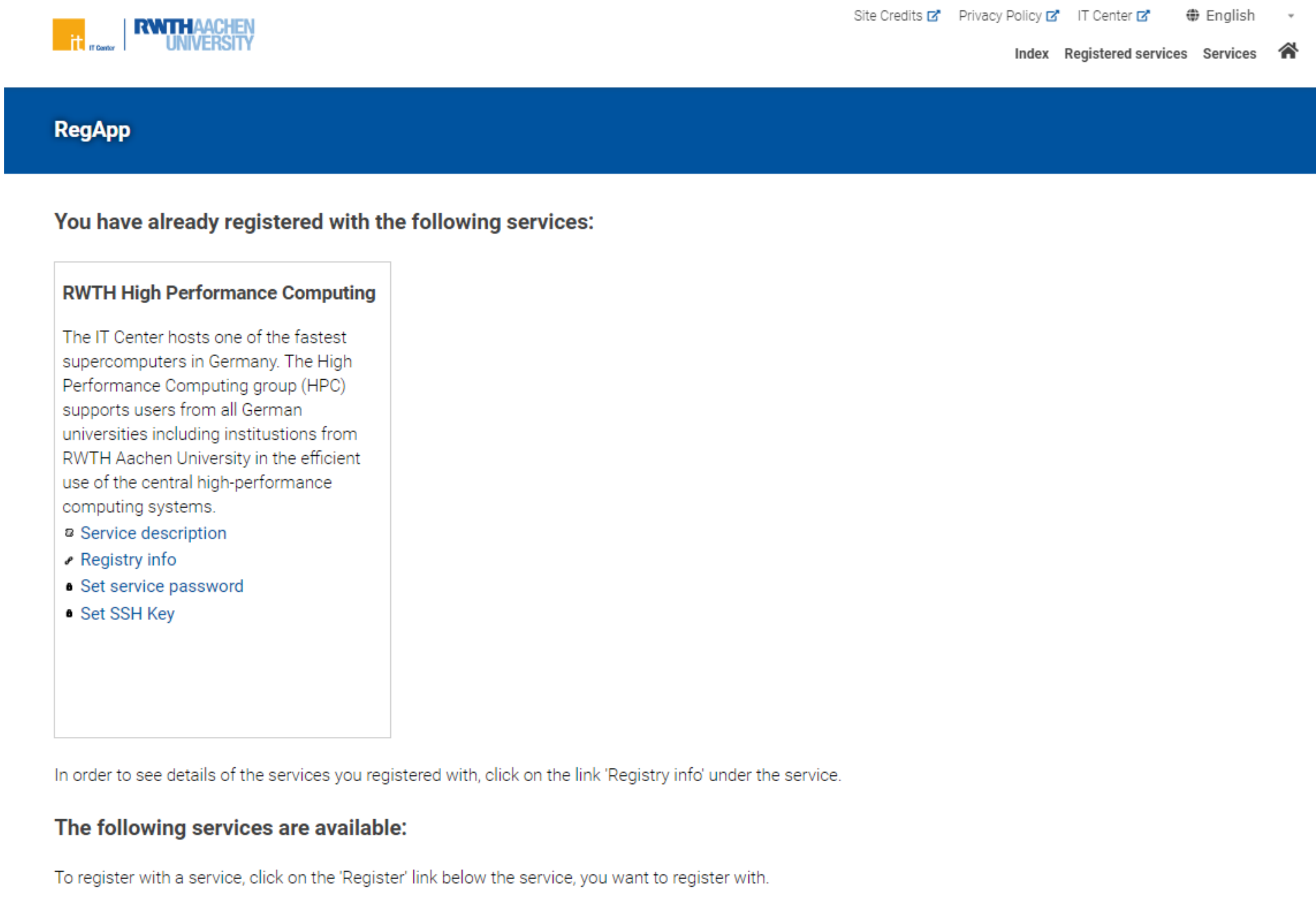
Welcome

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.

Remember Home organisation:	□
Federation:	All
Search filter:	
Home organization:	RWTH Aachen University

1. Login to RegApp

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



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.

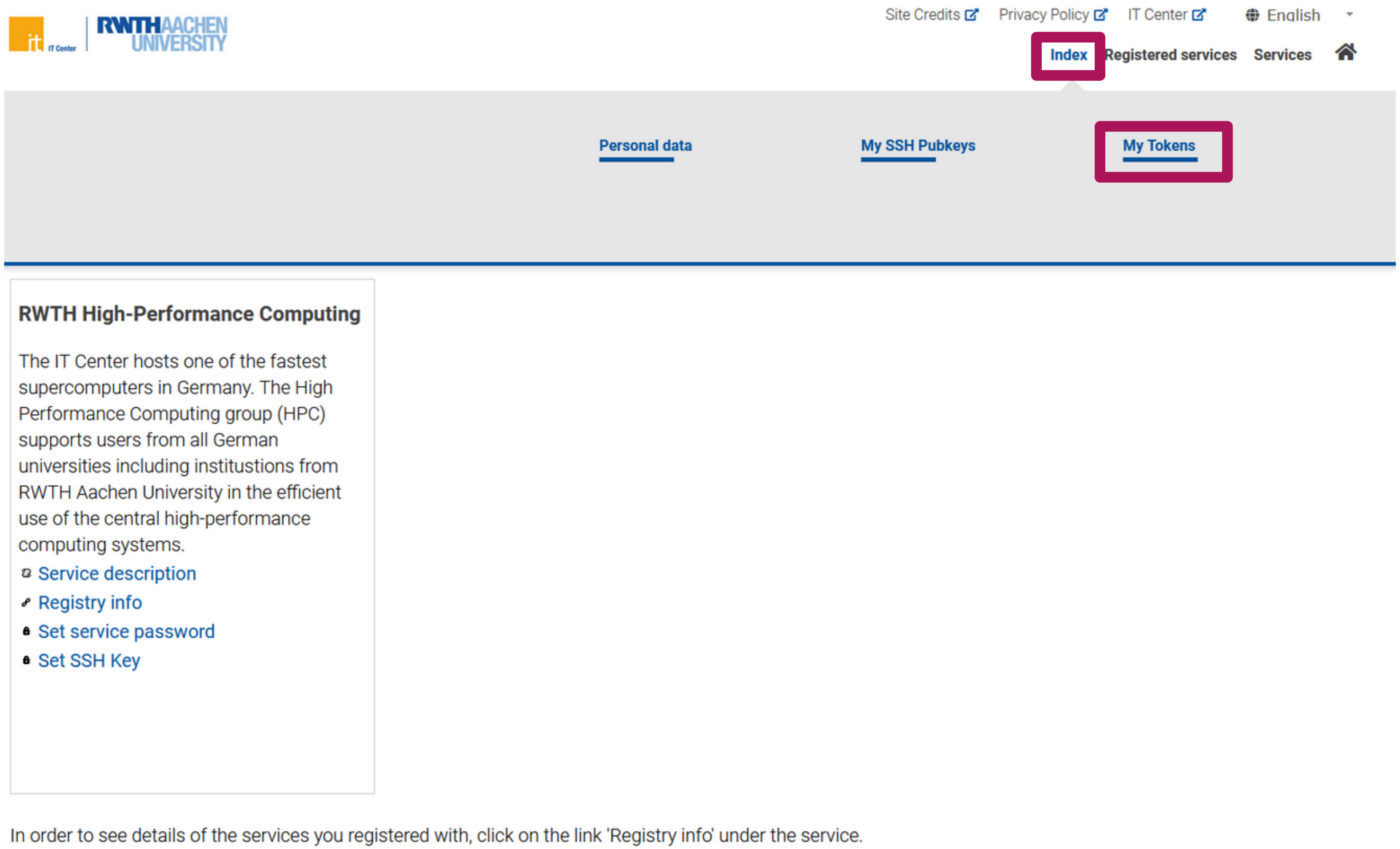
The following services are available:

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

2. Add Token to Account

- Only possible if you already have an HPC account

- Navigate to **Index → My Tokens** (German: **Übersicht → Meine Tokens**)



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.

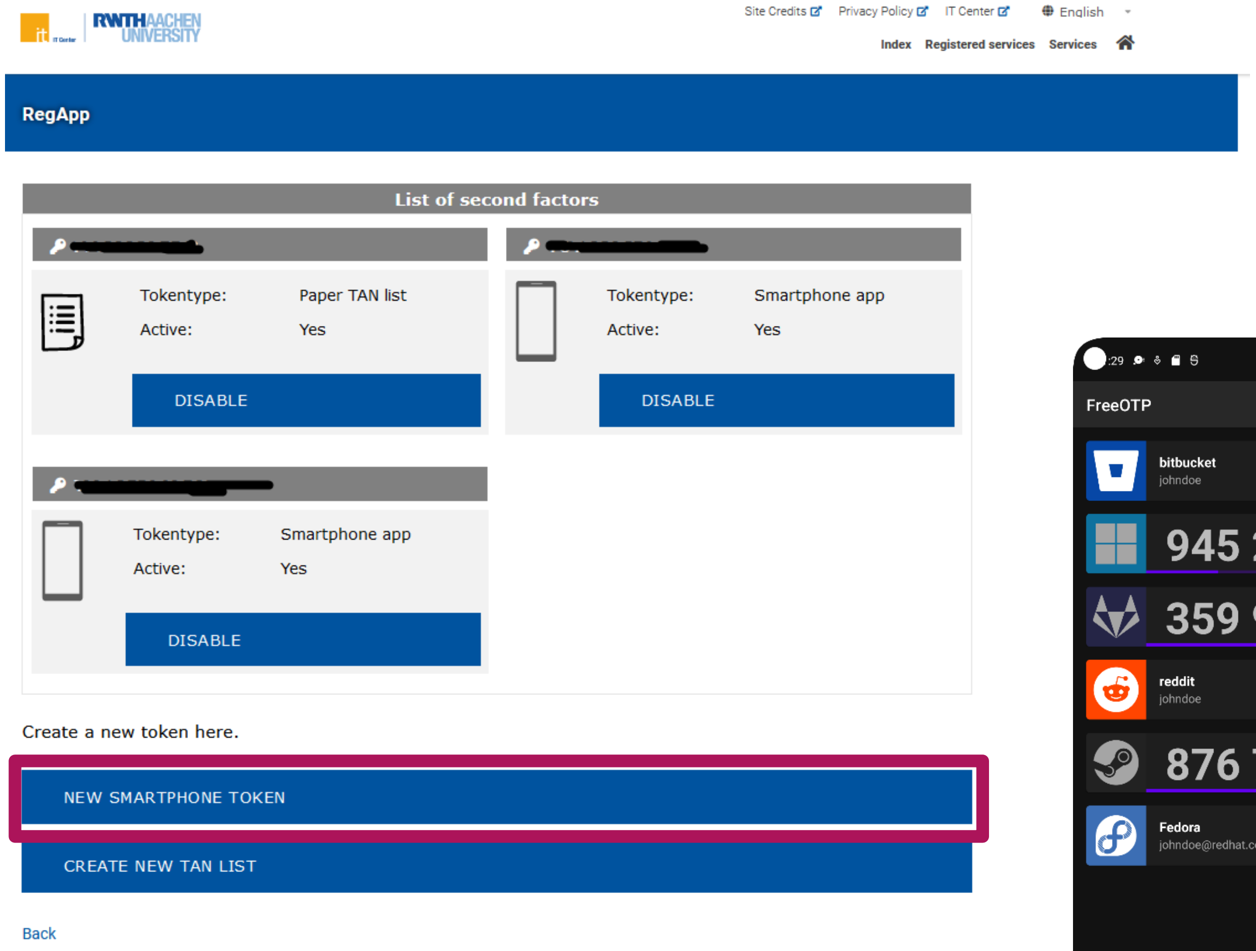
- Service description
- Registry info
- Set service password
- Set SSH Key

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

2. Add Token to Account

HPC.NRW

- 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



List of second factors

[redacted]

Tokentype:	Paper TAN list
Active:	Yes

DISABLE

[redacted]

Tokentype:	Smartphone app
Active:	Yes

DISABLE

[redacted]

Tokentype:	Smartphone app
Active:	Yes

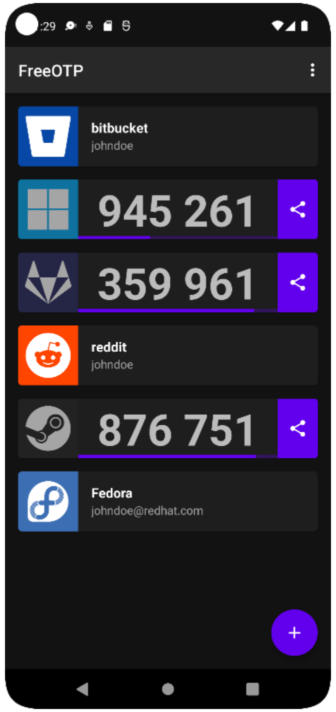
DISABLE

Create a new token here.

NEW SMARTPHONE TOKEN

CREATE NEW TAN LIST

Back



2. Add Token to Account

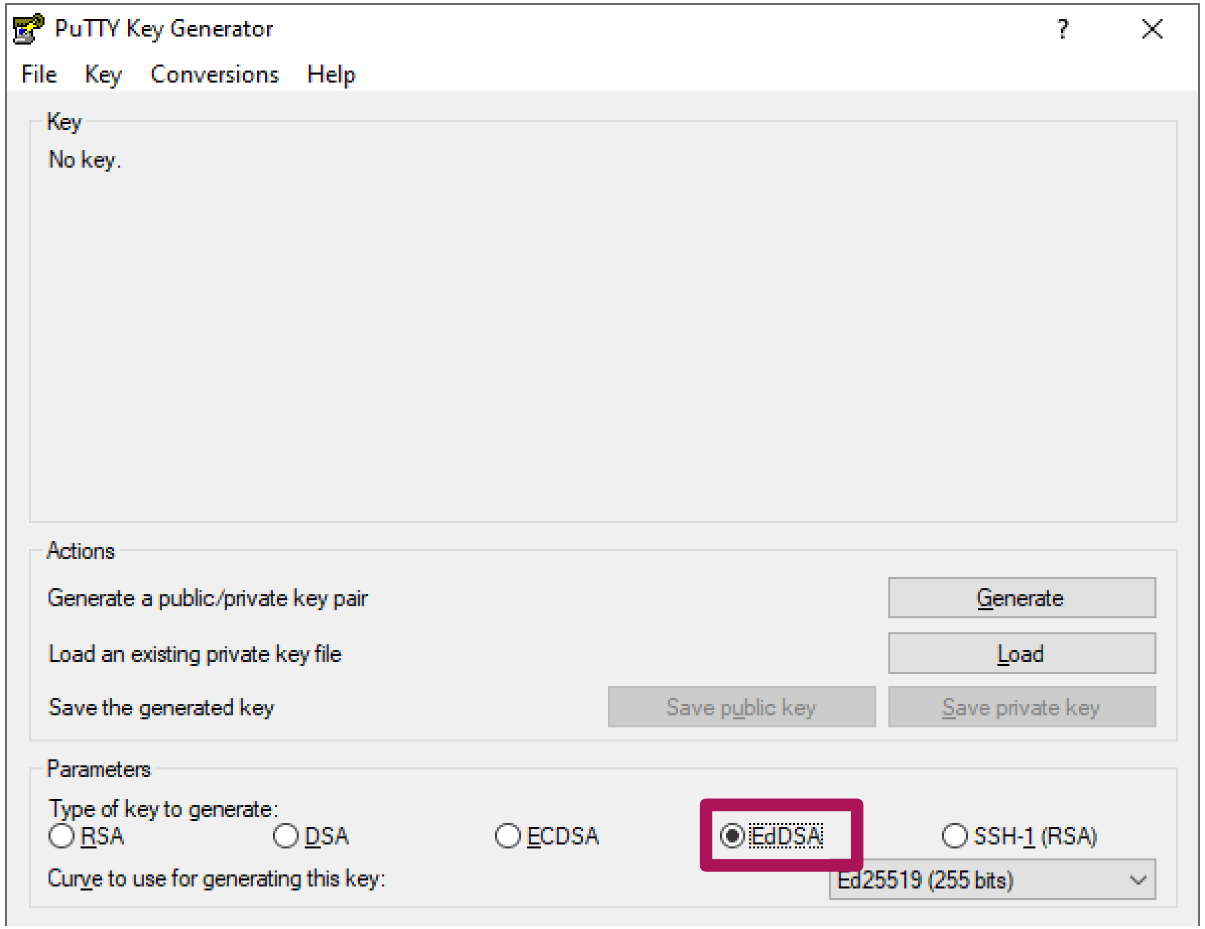
- Login using MFA now possible already (step 5)
- Disadvantage: You need the second factor for every login attempt now
- To avoid this: Use SSH key pairs associated with your account
- Then: Second factor only once every 10 hours required

3. Upload a public SSH key

HPC.NRW

- Generate a SSH Key Pair (if have not done before)
  - We recomment 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
```



PuTTY Key Generator

Key

No key.

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

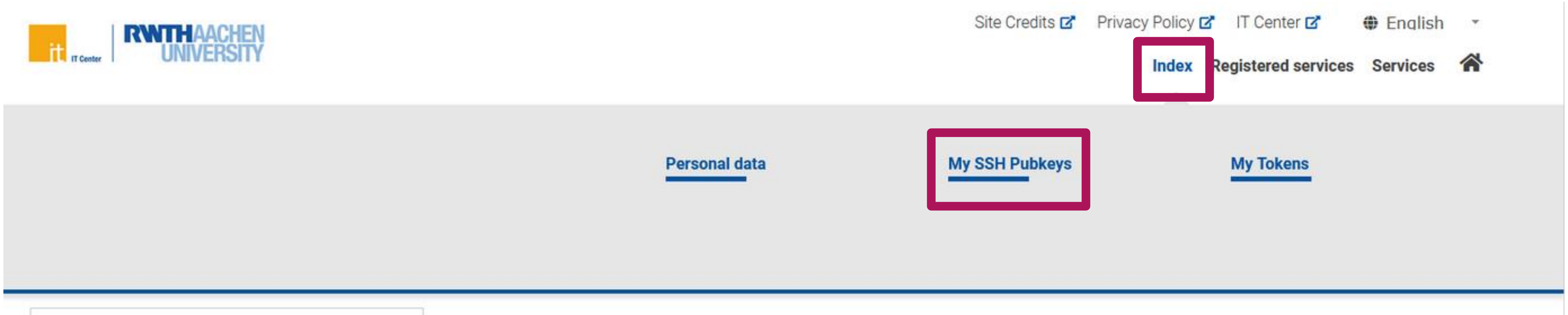
Type of key to generate:

○ RSA ○ DSA ○ ECDSA ● EdDSA ○ SSH-1 (RSA)

Curve to use for generating this key: Ed25519 (255 bits)

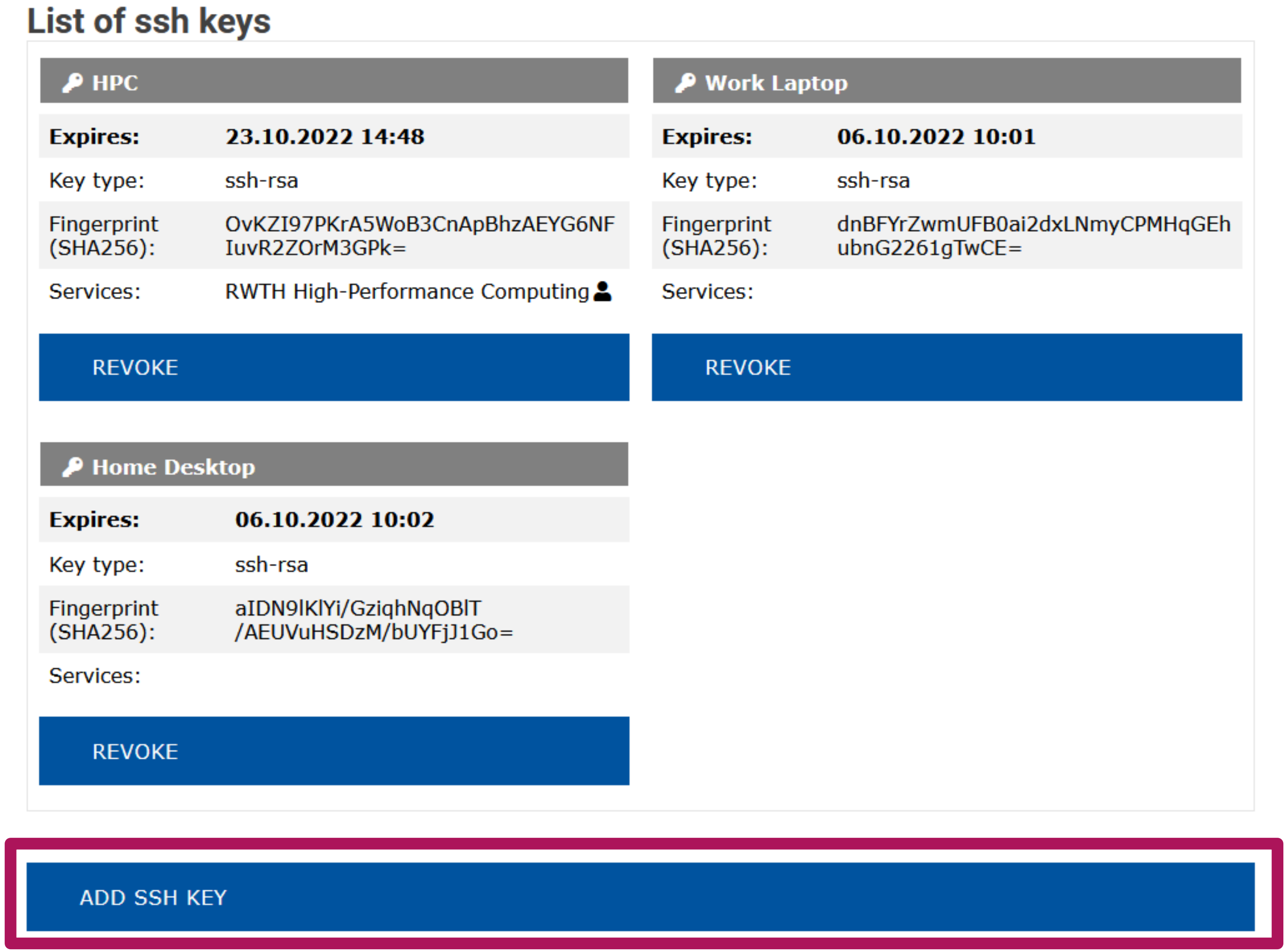
3. Upload a public SSH key

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



3. Upload a public SSH key

- Click **Add SSH Key**



List of ssh keys

HPC

Expires:	**23.10.2022 14:48**
Key type:	ssh-rsa
Fingerprint (SHA256):	OvKZI97PKrA5WoB3CnApBhzAEYG6NF IuvR2ZOrM3GPk=
Services:	RWTH High-Performance Computing 👤

REVOKE

Work Laptop

Expires:	**06.10.2022 10:01**
Key type:	ssh-rsa
Fingerprint (SHA256):	dnBFYrZwmUFB0ai2dxLNmyCPMHqGEh ubnG2261gTwCE=
Services:	

REVOKE

Home Desktop

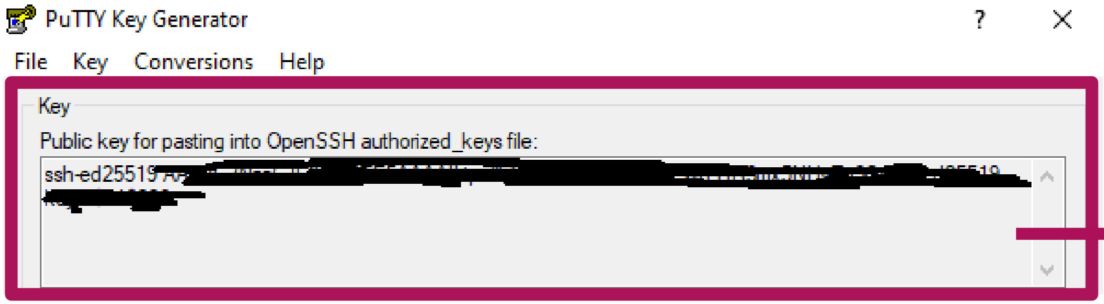
Expires:	**06.10.2022 10:02**
Key type:	ssh-rsa
Fingerprint (SHA256):	aIDN9lKlYi/GziqhNqOBlT /AEUVuHSDzM/bUYFjJ1Go=
Services:	

REVOKE

ADD SSH KEY

3. Upload a public SSH key

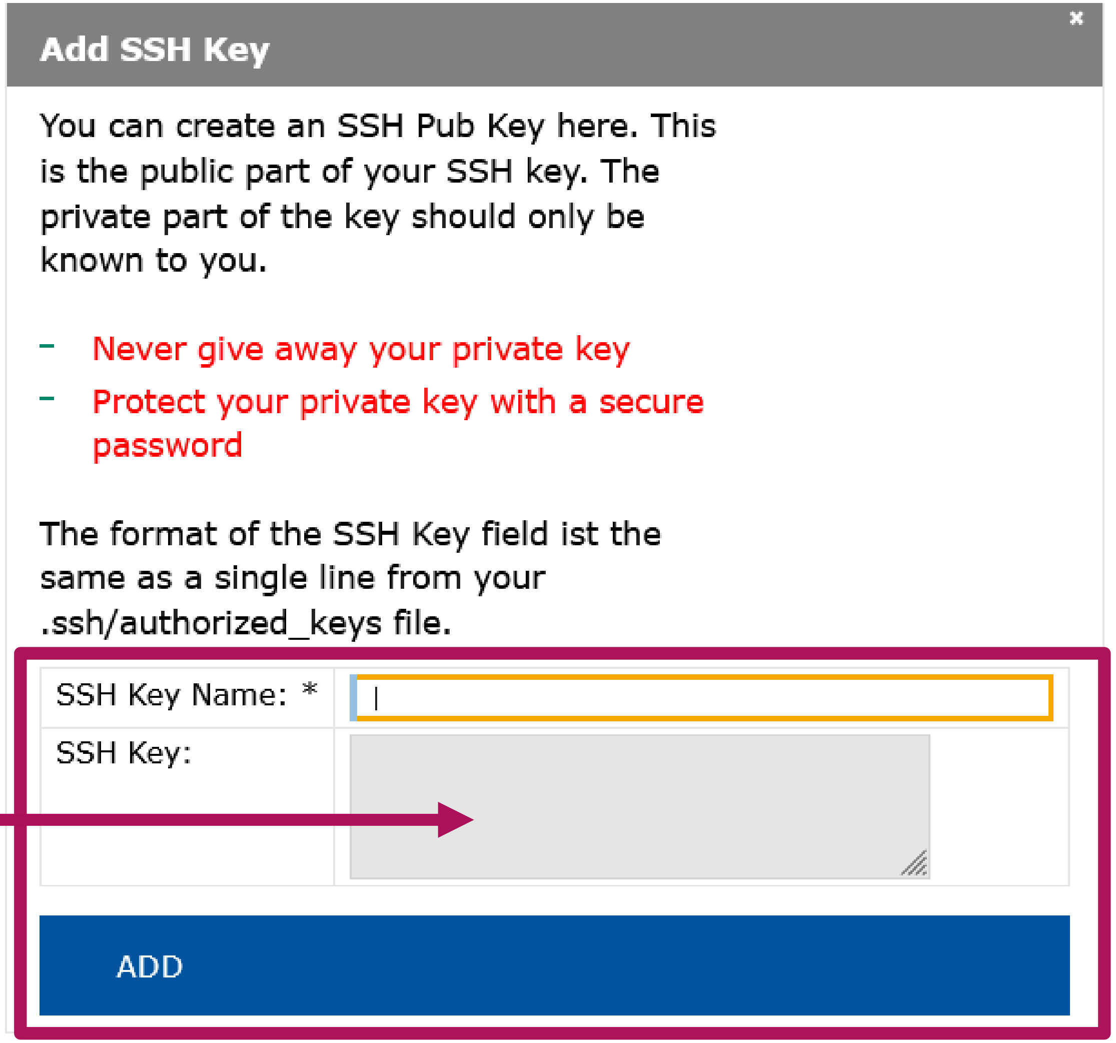
- Name the SSH Key
- Linux
  - Open public key (file ending „*.pub“)
  - Copy & paste key sequence to the text box
- Windows:
  - PuTTY uses different public key format
  - Open PuTTY Key Generator
  - Load key (if panel already closed)
  - Copy from “Public key for pasting into OpenSSH authorized_key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



Public key for pasting into OpenSSH authorized_keys file:

ssh-ed25519 [redacted]

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



You can create an SSH Pub Key here. This is the public part of your SSH key. The private part of the key should only be known to you.

- Never give away your private key
- Protect your private key with a secure password

The format of the SSH Key field ist the same as a single line from your .ssh/authorized_keys file.

SSH Key Name: *

SSH Key:

4. Assign SSH Key to Service HPC

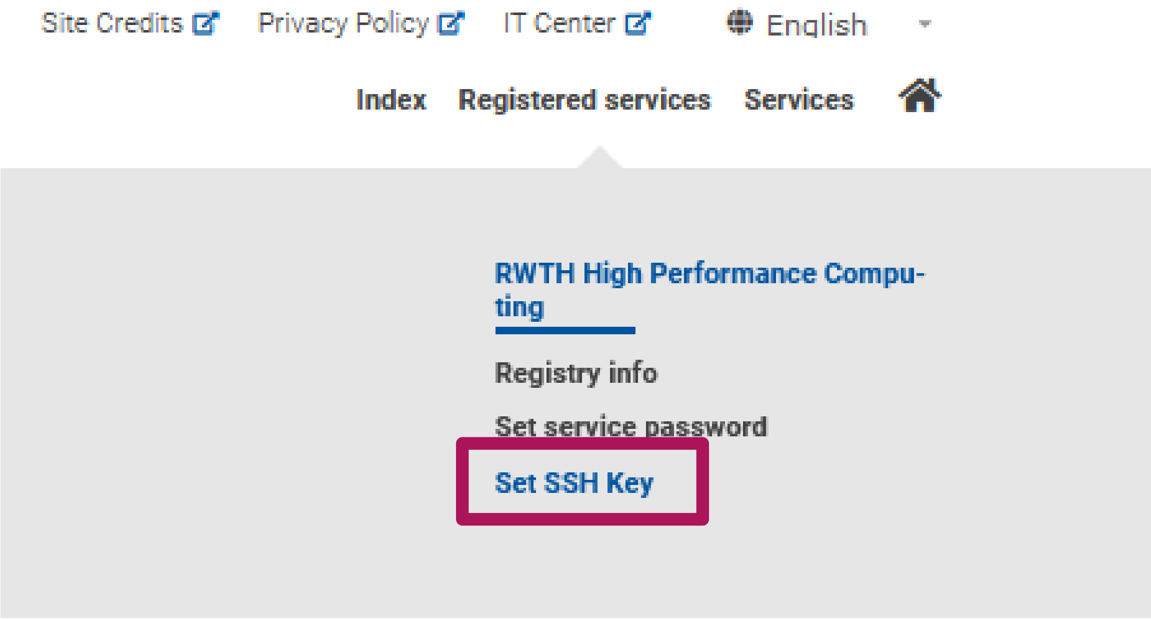
- Navigate to **Registered Services → RWTH High Performance Computing → Set SSH Key**

- 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

5. Log In to a MFA Node

- Conntect to the RWTH VPN / use “trusted” network

- Login per native ssh, PuTTY, WSL or FastX possible

- 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`

- CLAIX-2023 dialog nodes coming soon:
  `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`

- 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

HPC.NRW

Example 1: ssh via commandline

```
name@local: $ ssh –l ab12345 login18-1.hpc.itc.rwth-aachen.de
```

5. Log In to a MFA Node

Example 1: ssh via commandline

```
name@local: $ ssh –l ab12345 login18-1.hpc.itc.rwth-aachen.de
The authenticity of host 'login18-1.hpc.itc.rwth-aachen.de (134.61.193.179)' 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 login18-1.hpc.itc.rwth-aachen.de
The authenticity of host 'login18-1.hpc.itc.rwth-aachen.de (134.61.193.179)' 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

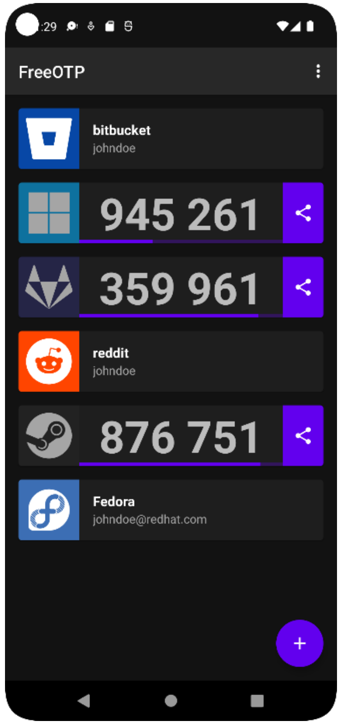
Example 1: ssh via commandline

```
name@local: $ ssh –l ab12345 login18-1.hpc.itc.rwth-aachen.de
The authenticity of host 'login18-1.hpc.itc.rwth-aachen.de (134.61.193.179)' 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 'login18-1.hpc.itc.rwth-aachen.de,134.61.193.179' (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 login18-1.hpc.itc.rwth-aachen.de
The authenticity of host 'login18-1.hpc.itc.rwth-aachen.de (134.61.193.179)' 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 'login18-1.hpc.itc.rwth-aachen.de,134.61.193.179' (ECDSA) to the list of known hosts.
Password: ********
Two-factor code:
```

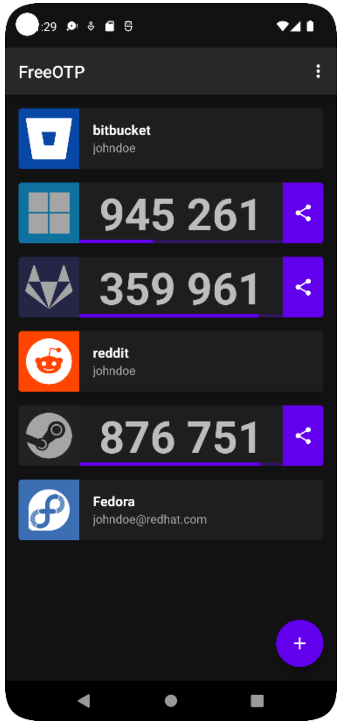


5. Log In to a MFA Node

HPC.NRW

Example 1: ssh via commandline

```
name@local: $ ssh –l ab12345 login18-1.hpc.itc.rwth-aachen.de
The authenticity of host 'login18-1.hpc.itc.rwth-aachen.de (134.61.193.179)' 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 'login18-1.hpc.itc.rwth-aachen.de,134.61.193.179' (ECDSA) to the list of known hosts.
Password: ********
Two-factor code: ******
```



5. Log In to a MFA Node

HPC.NRW

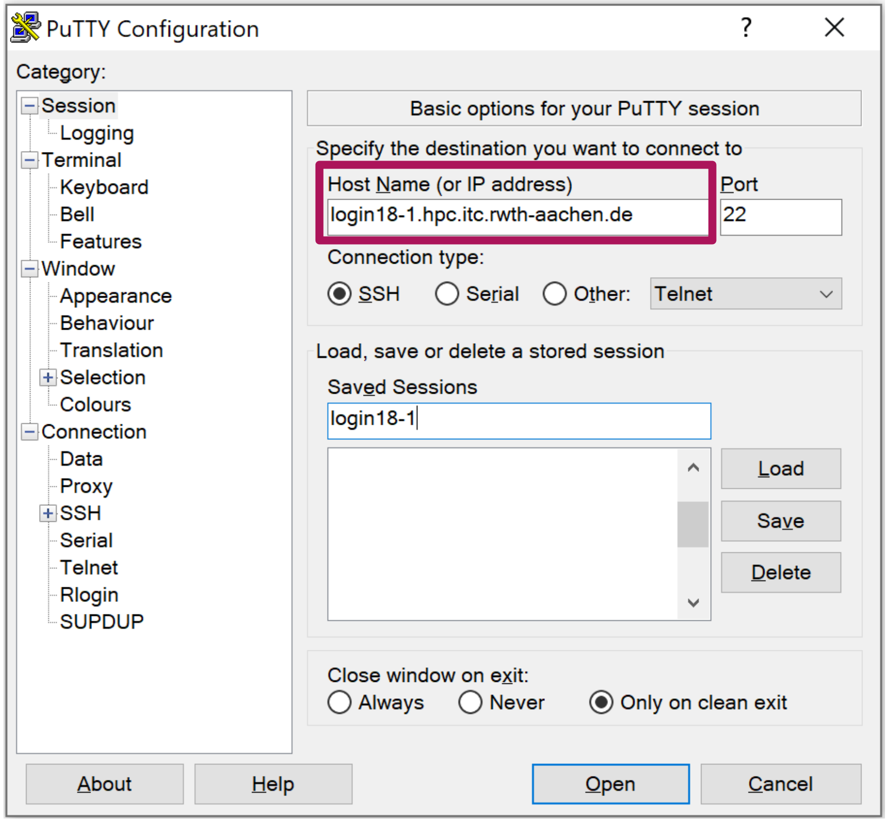
Example 1: ssh via commandline

```
name@local: $ ssh -l ab12345 login18-1.hpc.itc.rwth-aachen.de
The authenticity of host 'login18-1.hpc.itc.rwth-aachen.de (134.61.193.179)' 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 'login18-1.hpc.itc.rwth-aachen.de,134.61.193.179' (ECDSA) to the list of known hosts.
Password: ********
Two-factor code: ******
Last login: Mon Jan 22 14:27:05 2024 from local.someinstitute.itc.rwth-aachen.de
                \_\_\_\_  \_  \_\_\_\_\_  \_   Rheinisch-
                \_   \_\_ \__ \_  \_  \_  \_   Westfaelische
                \_\_\_  \_\_\_\_  \_  \_\_\_   Technische
                \_  \_   \__ \__  \_  \_  \_   Hochschule
                \_   \_   \_  \_  \_  \_  \_   Aachen
                ============================================
                                                   IT Center
*******************************************************************************
* User documentation:      https://www.itc.rwth-aachen.de/hpc-doc             *
* HPC wiki:                https://hpc-wiki.info                              *
* HPC trainings:           https://blog.rwth-aachen.de/itc-events             *
* Changelog:               https://blog.rwth-aachen.de/itc-changelog          *
* Support:                 mailto:servicedesk@itc.rwth-aachen.de              *
*******************************************************************************

You are connected to the node 'login18-1' (operating system: LINUX, ROCKY 8.9).

ab123456@login18-1 ~ $
```

5. Log In to a MFA Node

Example 2: PuTTY

1. Open “PuTTY”.
2. Specify a host name, e.g. “login18-1.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



Specify the destination you want to connect to

Host Name (or IP address): login18-1.hpc.itc.rwth-aachen.de

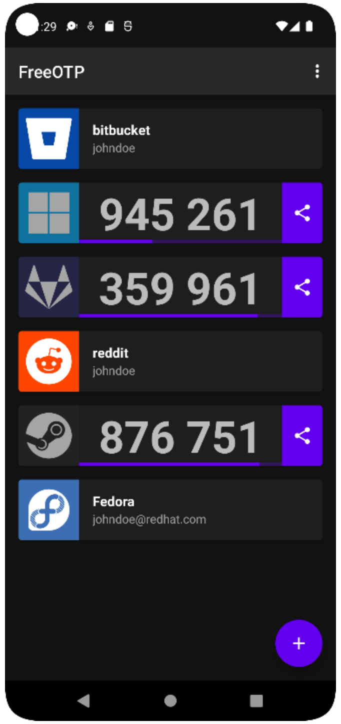
Port: 22

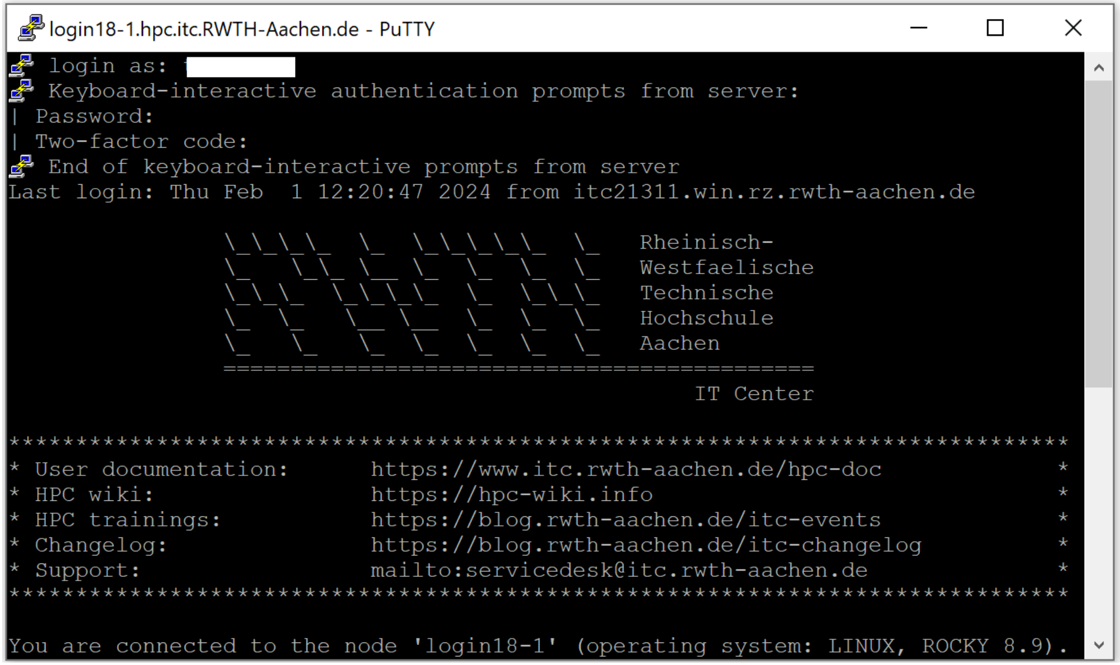
Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions: login18-1

Close window on exit: ○ Always ○ Never ● Only on clean exit



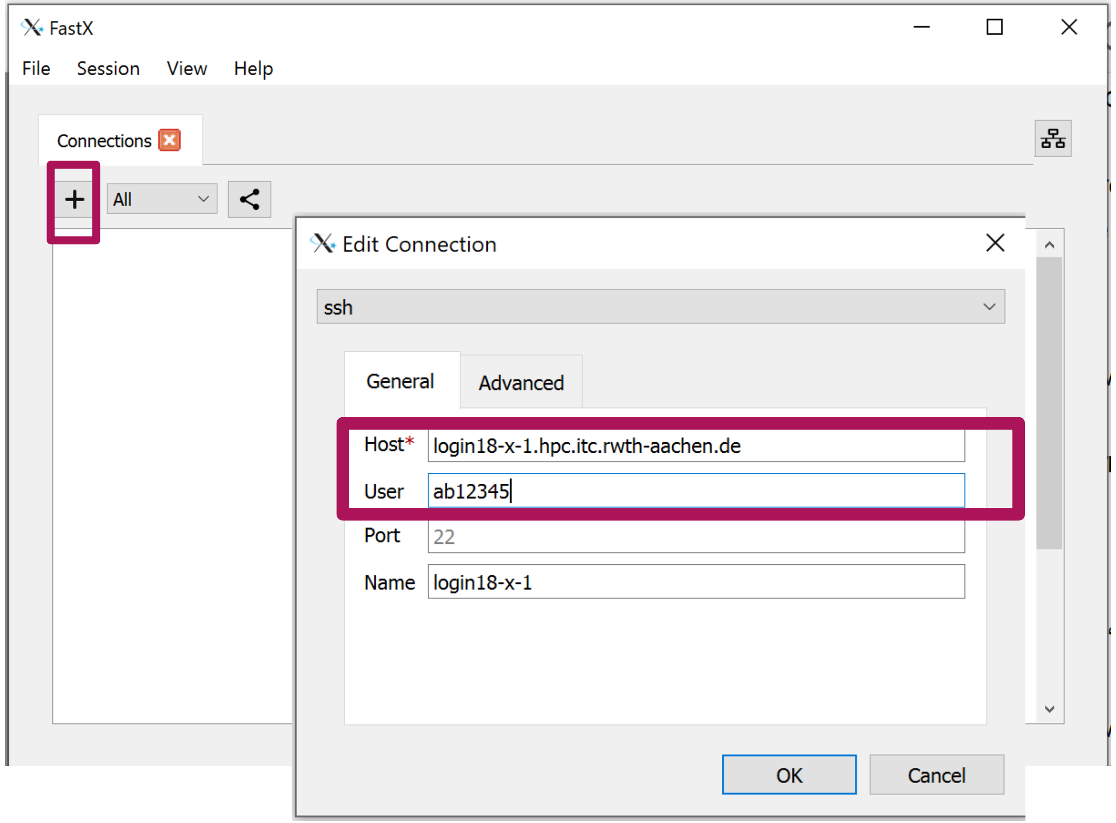


```
 login as: [redacted]
 Keyboard-interactive authentication prompts from server:
| Password:
| Two-factor code:
 End of keyboard-interactive prompts from server
Last login: Thu Feb  1 12:20:47 2024 from itc21311.win.rz.rwth-aachen.de

                \_\_\_\_  \_  \_\_\_\_\_  \_   Rheinisch-
                \_   \_\_ \__ \_  \_  \_  \_   Westfaelische
                \_\_\_  \_\_\_\_  \_  \_\_\_   Technische
                \_  \_   \__ \__  \_  \_  \_   Hochschule
                \_   \_   \_  \_  \_  \_  \_   Aachen
                ============================================
                                                   IT Center

********************************************************************************
* User documentation:      https://www.itc.rwth-aachen.de/hpc-doc              *
* HPC wiki:                https://hpc-wiki.info                               *
* HPC trainings:           https://blog.rwth-aachen.de/itc-events              *
* Changelog:               https://blog.rwth-aachen.de/itc-changelog           *
* Support:                 mailto:servicedesk@itc.rwth-aachen.de               *
********************************************************************************

You are connected to the node 'login18-1' (operating system: LINUX, ROCKY 8.9).
```

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. login18-x-1.hpc.itc.rwth-aachen.de as host



ssh

Host* login18-x-1.hpc.itc.rwth-aachen.de

User ab12345

Port 22

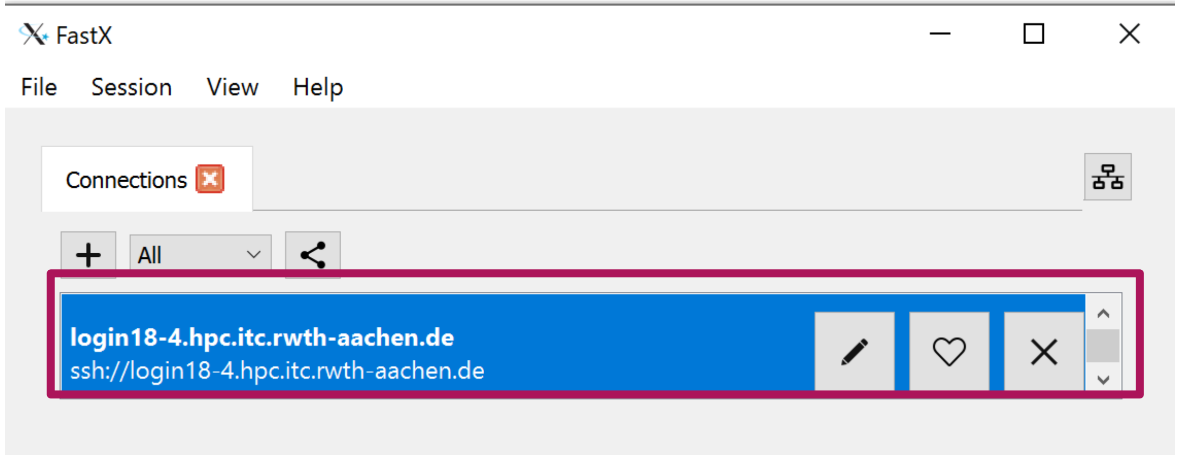
Name login18-x-1

5. Log In to a MFA Node

HPC.NRW

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. login18-x-1.hpc.itc.rwth-aachen.de as host**
6. **Double click on new connection**

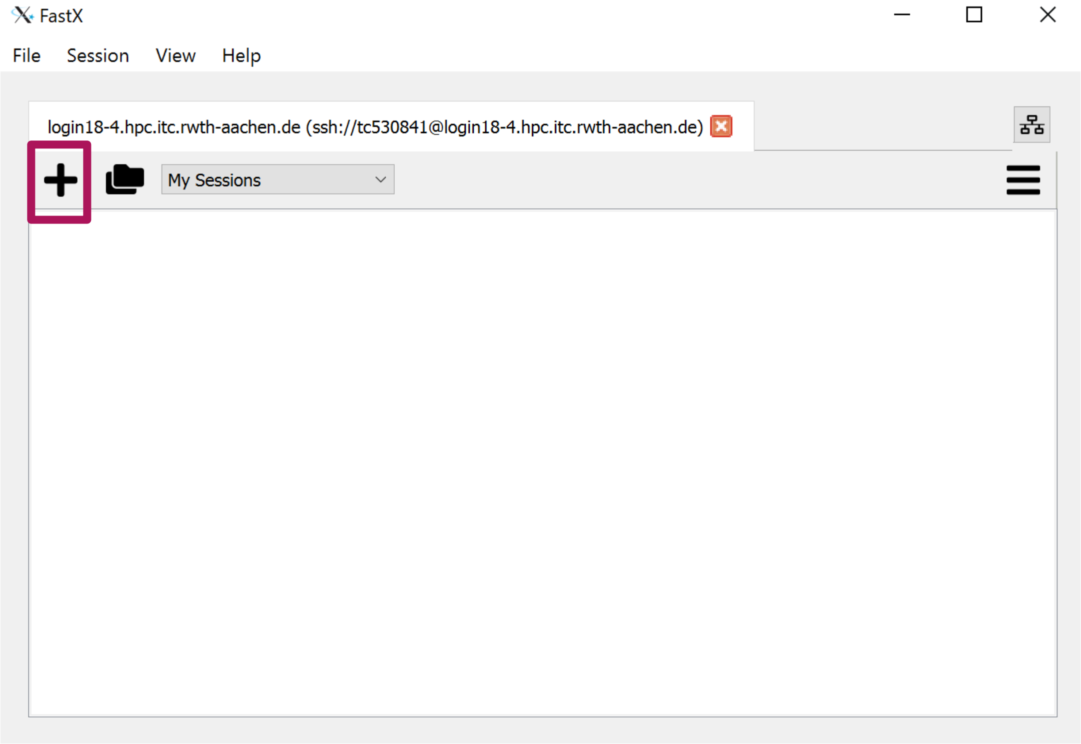


login18-4.hpc.itc.rwth-aachen.de
ssh://login18-4.hpc.itc.rwth-aachen.de

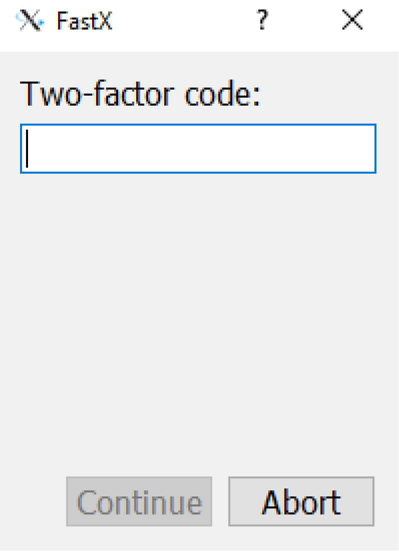
5. Log In to a MFA Node

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. login18-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



login18-4.hpc.itc.rwth-aachen.de (ssh://tc530841@login18-4.hpc.itc.rwth-aachen.de)

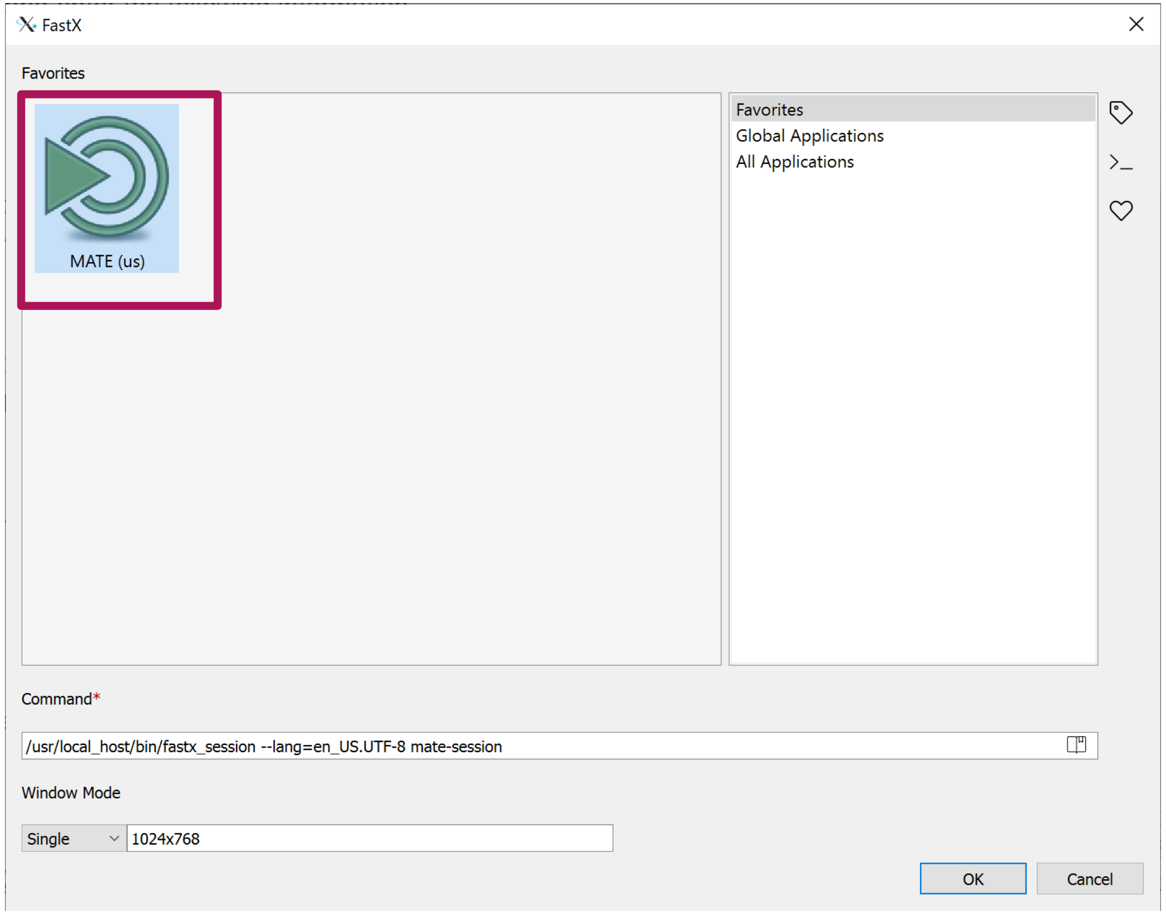


Two-factor code:

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. login18-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)



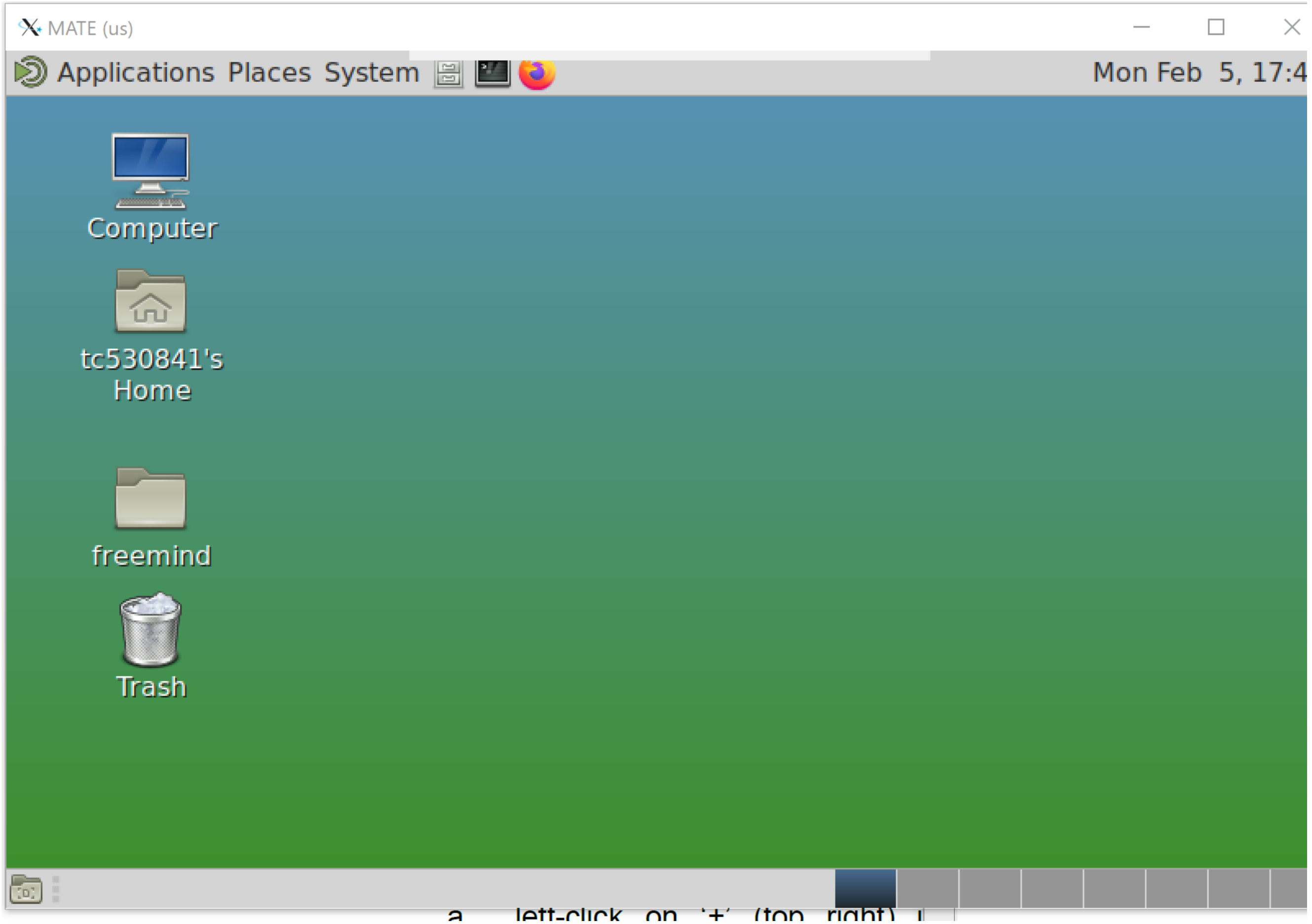
Command*: /usr/local_host/bin/fastx_session --lang=en_US.UTF-8 mate-session

Window Mode: Single 1024x768

5. Log In to a MFA Node

Example 3: FastX

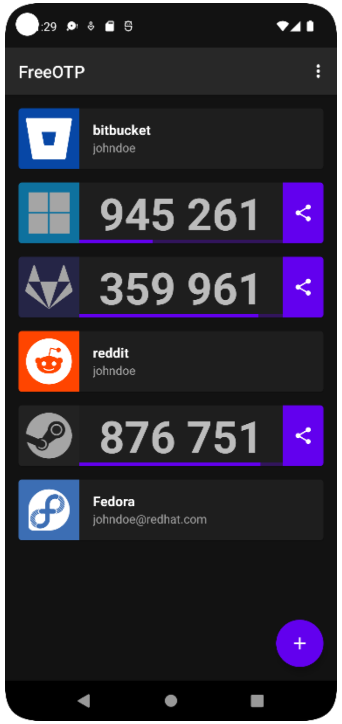
1. **Download here https://www.starnet.com/download/fastx-client**
2. **Open client**
3. **Click +**
4. **Select “ssh”**
5. **Use e.g. login18-x-1.hpc.itc.rwth-aachen.de**
6. **Double click on new connection**
7. **Click +**
8. **Type user name**
9. **Type password**
10. **Type two-factor code**
11. **Select an environment (e.g., MATE)**
12. **Use full graphical remote session**

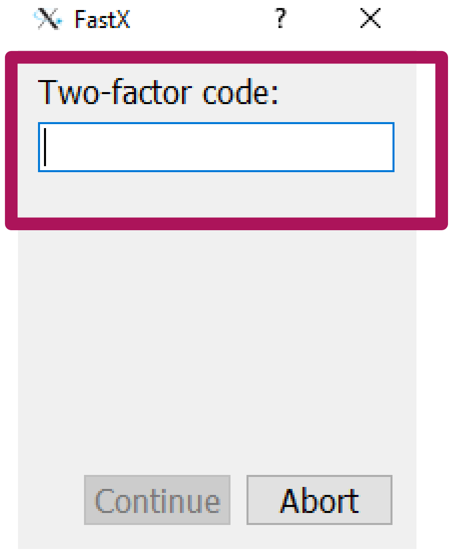


5. Log In to a MFA Node

Up to now:

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



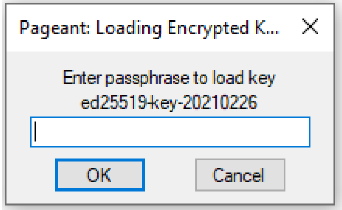


5. Log In to a MFA Node

- Key agents might support you
  - Linux

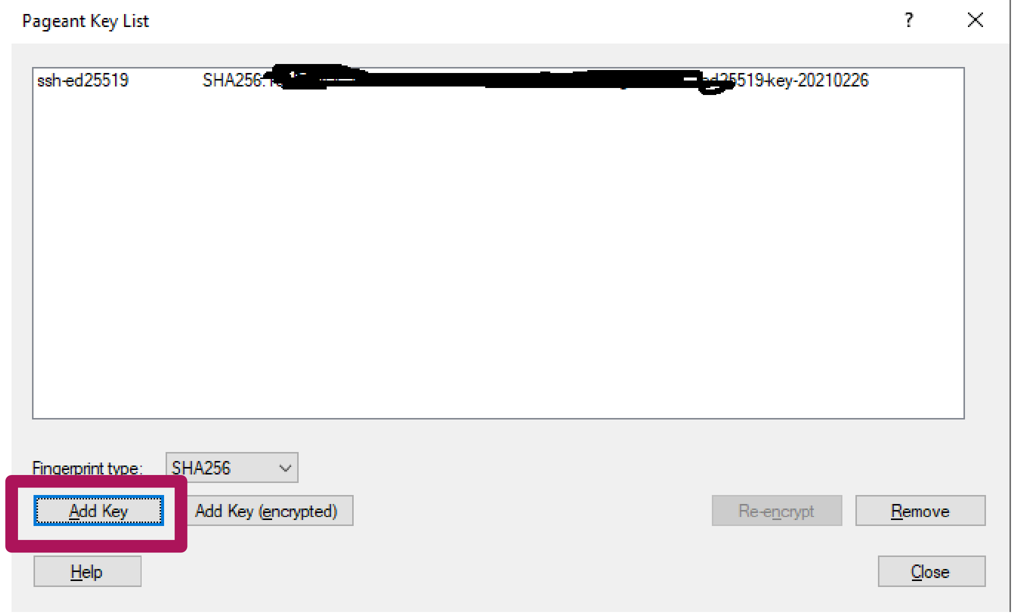
    ```
    $ eval `ssh-agent`
    $ ssh-add ~/.ssh/id_ed25519
    ```

  - Windows
    - Use PuTTY Pageant (also for login via FastX, WinSCP, etc.)



Pageant: Loading Encrypted K...

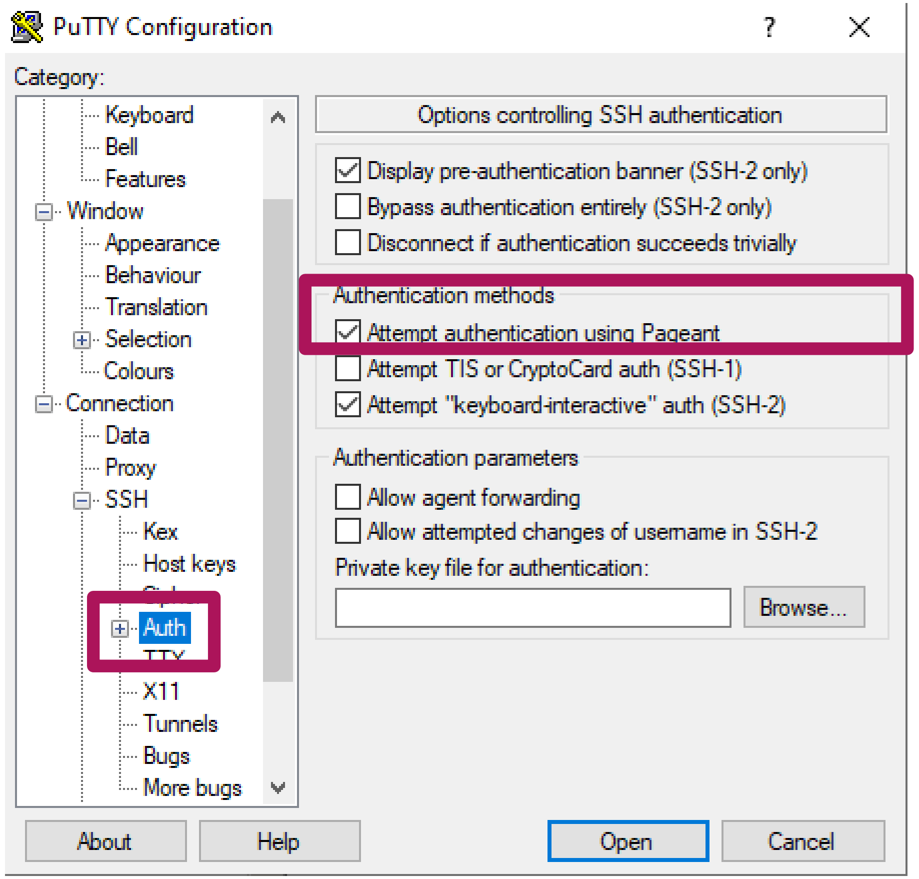
Enter passphrase to load key ed25519-key-20210226



Pageant Key List

ssh-ed25519 SHA256:[redacted]25519-key-20210226

Fingerprint type: SHA256



PuTTY Configuration

Category:

Options controlling SSH authentication

☑ Display pre-authentication banner (SSH-2 only)
☐ Bypass authentication entirely (SSH-2 only)
☐ Disconnect if authentication succeeds trivially

Authentication methods

☑ Attempt authentication using Pageant
☐ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

☐ Allow agent forwarding
☐ Allow attempted changes of username in SSH-2

Private key file for authentication:

Conclusion

HPC.NRW

- 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?