HPC.NRW

NHR4CES NHR for Computational Engineering Science

TECHNISCHE UNIVERSITÄT DARMSTADT

RWTH AACHEN UNIVERSITY

Using multi-factor authorization for CLAIX

Tim Cramer

GREAT COMPUTING COMES WITH GREAT SUPPORT.

RegApp and Multi-Factor Authentication

- 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 (voluntary at the moment)
    - 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)

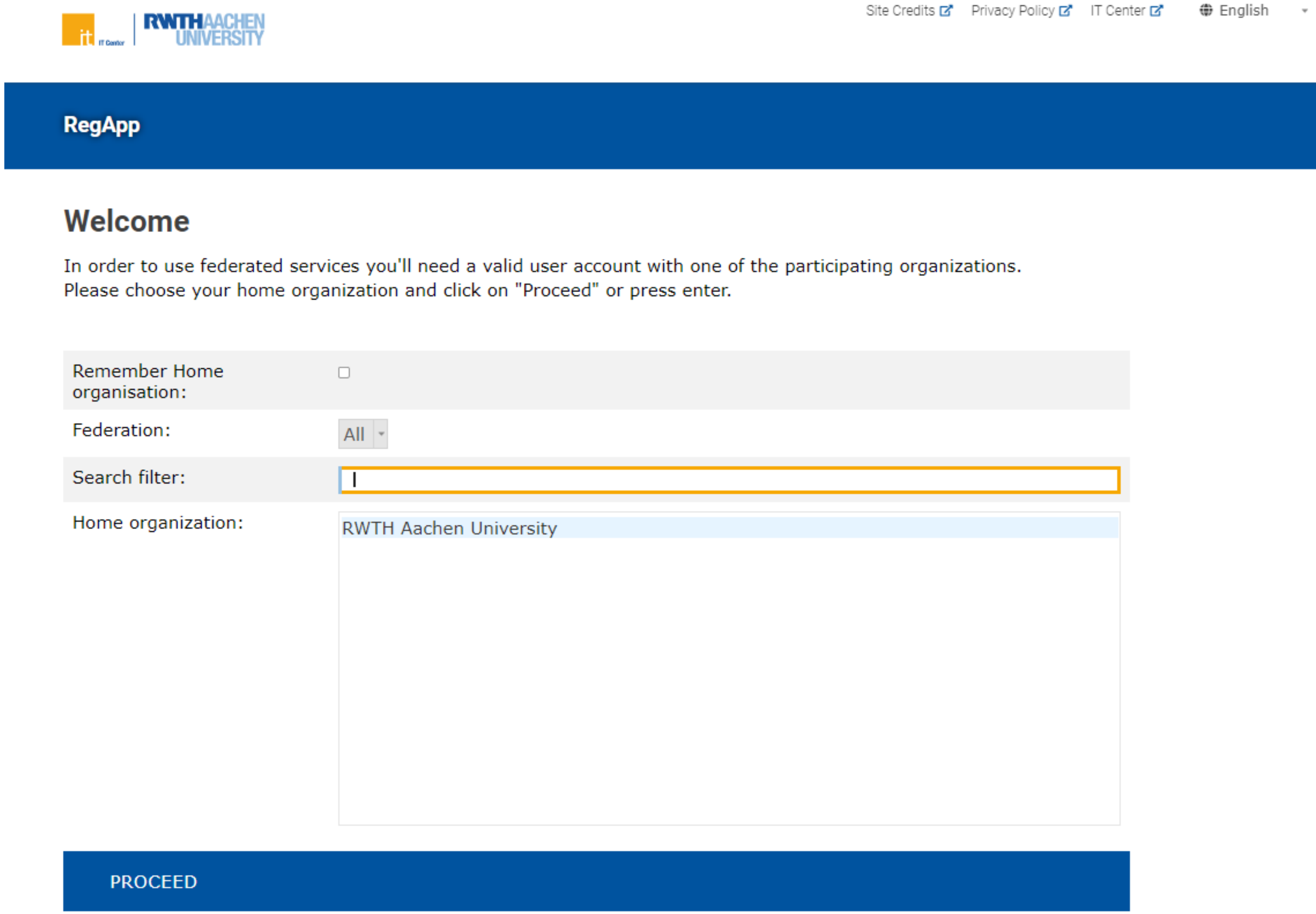
1. Login to RegApp
2. Add Token to Account
3. Upload a public SSH key
4. Assign SSH Key to Service HPC
5. Log In to a MFA Node

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.

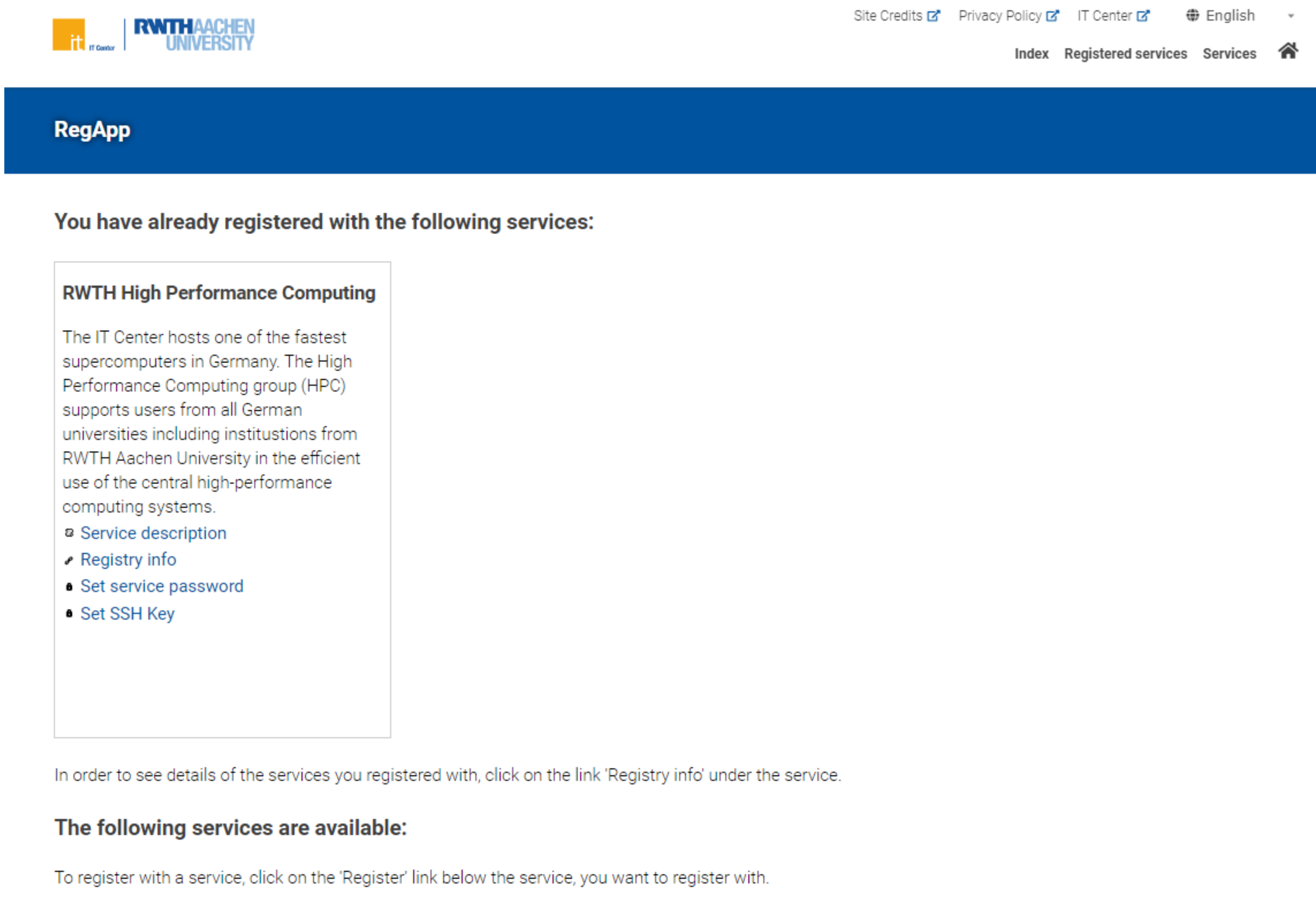
Remember Home organisation:	□
Federation:	All
Search filter:	
Home organization:	RWTH Aachen University

PROCEED

1. Login to RegApp

- After login you see the RegApp dashboard

- Currently only one service configured (HPC)



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.

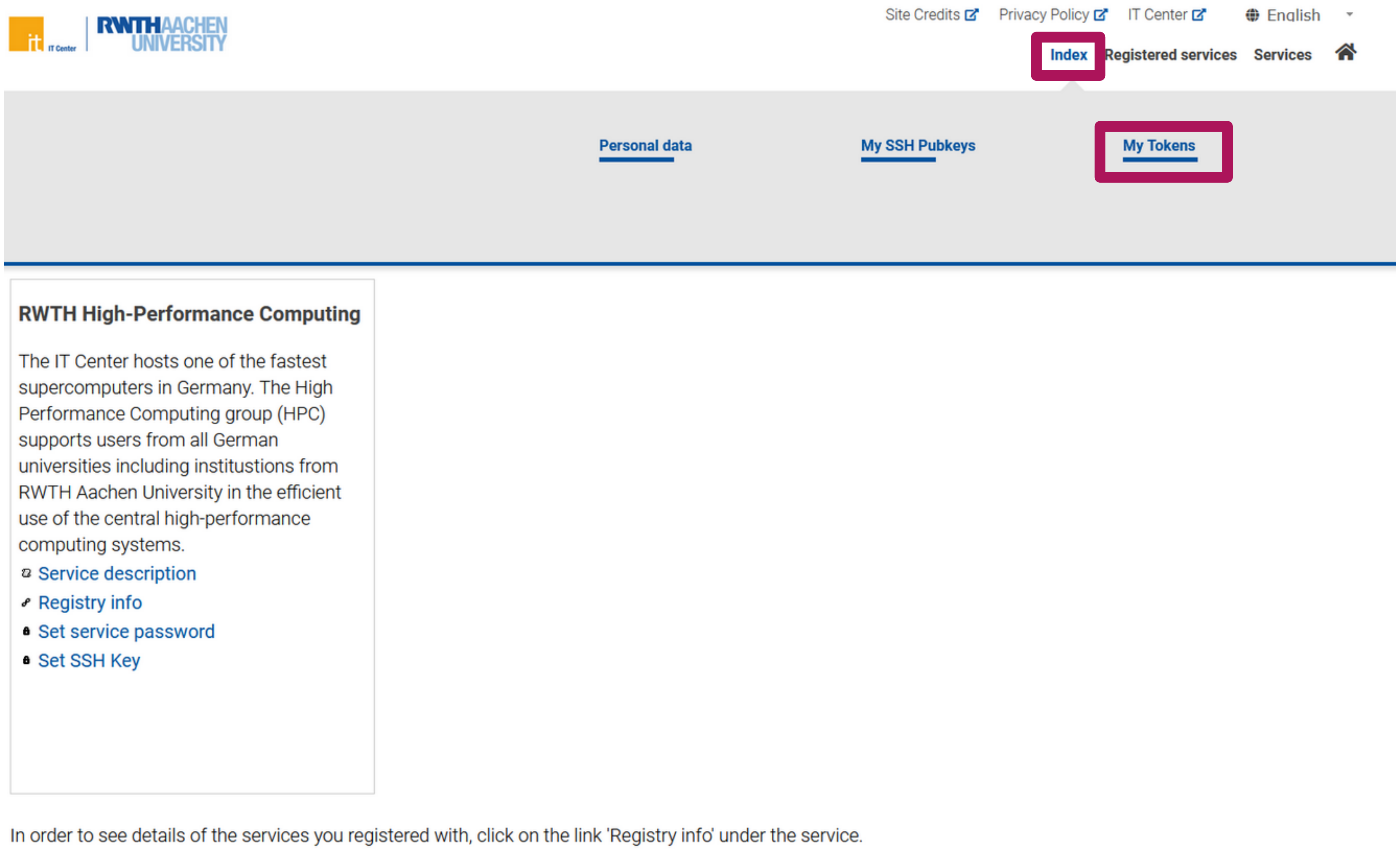
The following services are available:

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

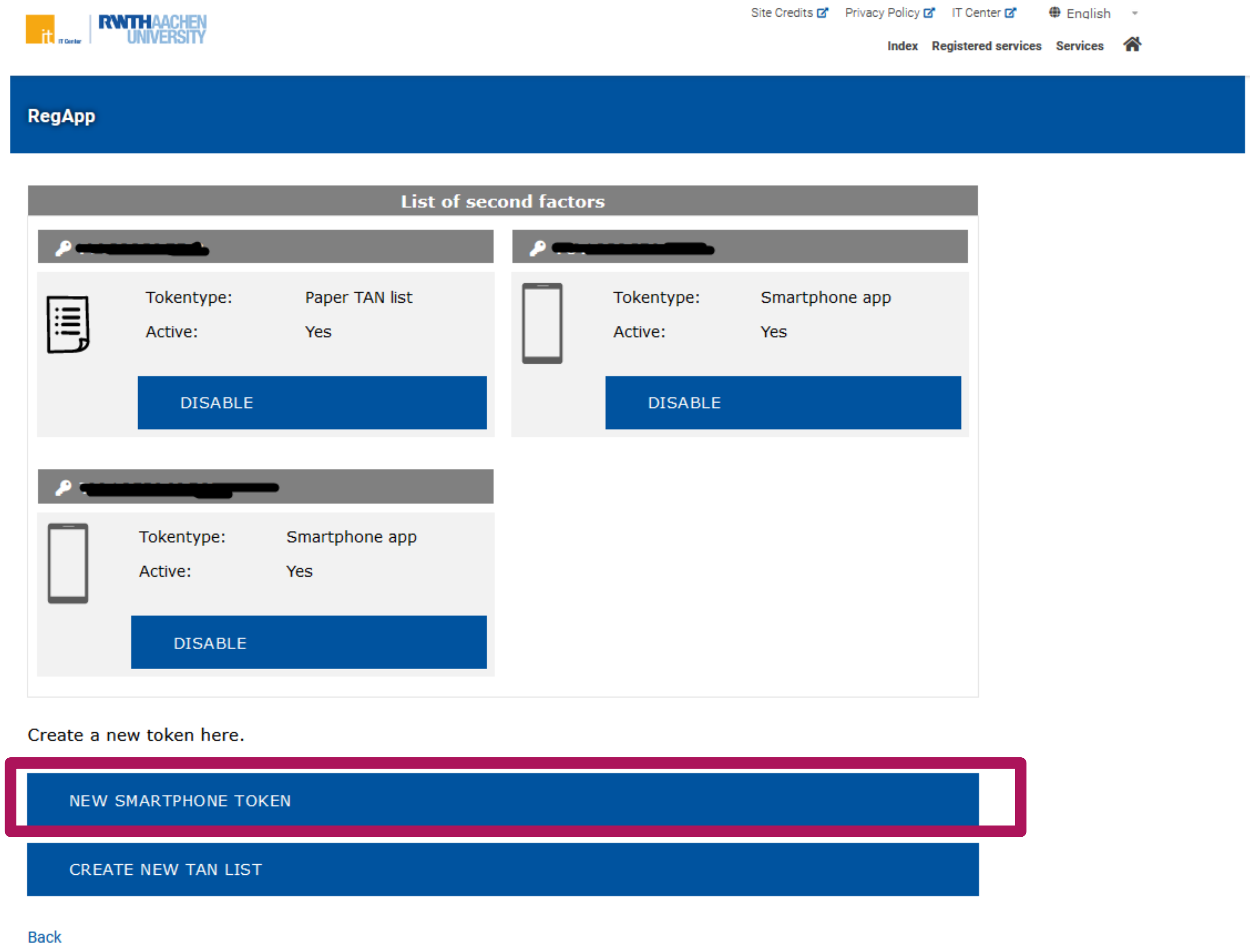
The IT Center hosts one of the fastest supercomputers in Germany. The High Performance Computing group (HPC) supports users from all German universities including institutions from RWTH Aachen University in the efficient use of the central high-performance computing systems.

- 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

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



Site Credits | Privacy Policy | IT Center | English

Index | Registered services | Services

RegApp

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

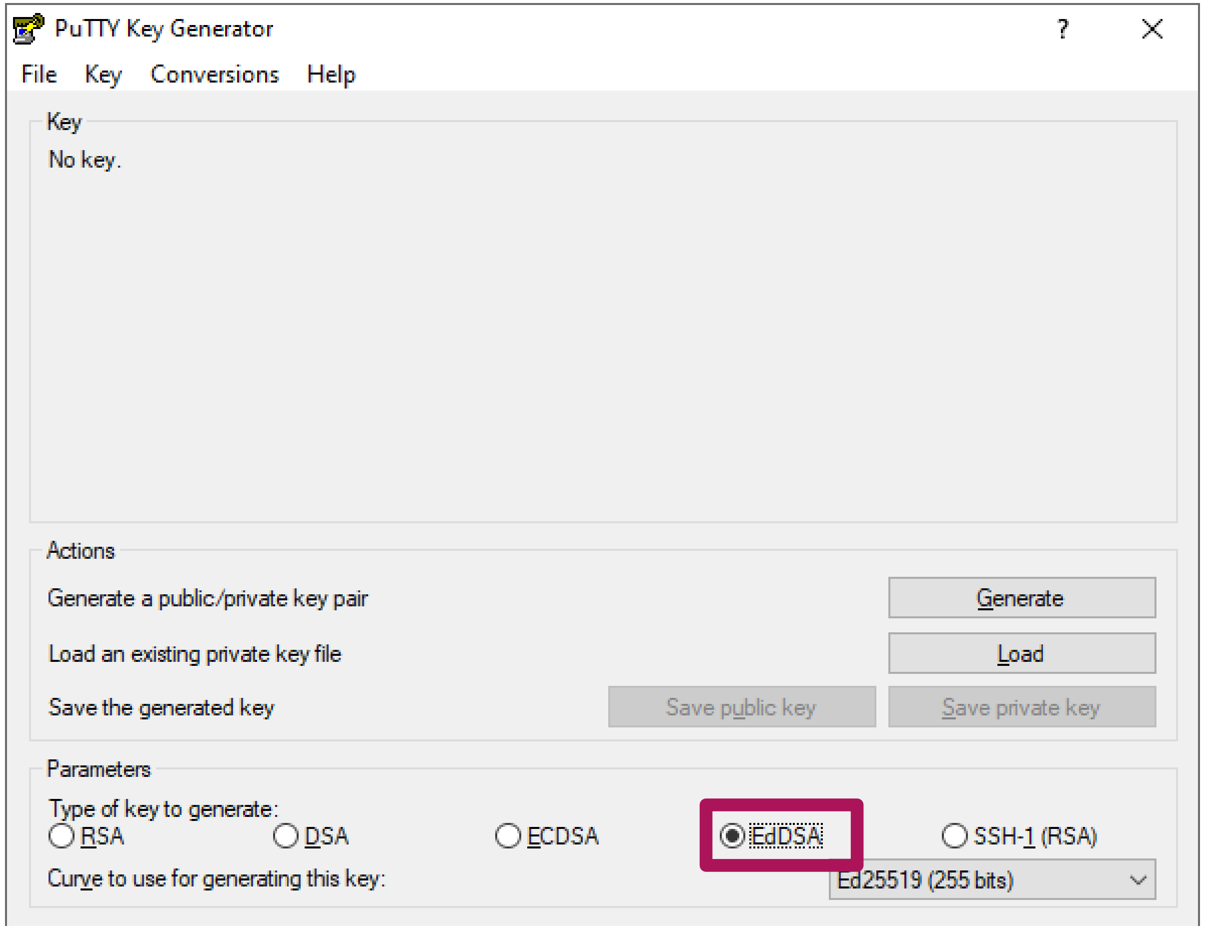
2. Add Token to Account

- 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

- 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
```



Key

No key.

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

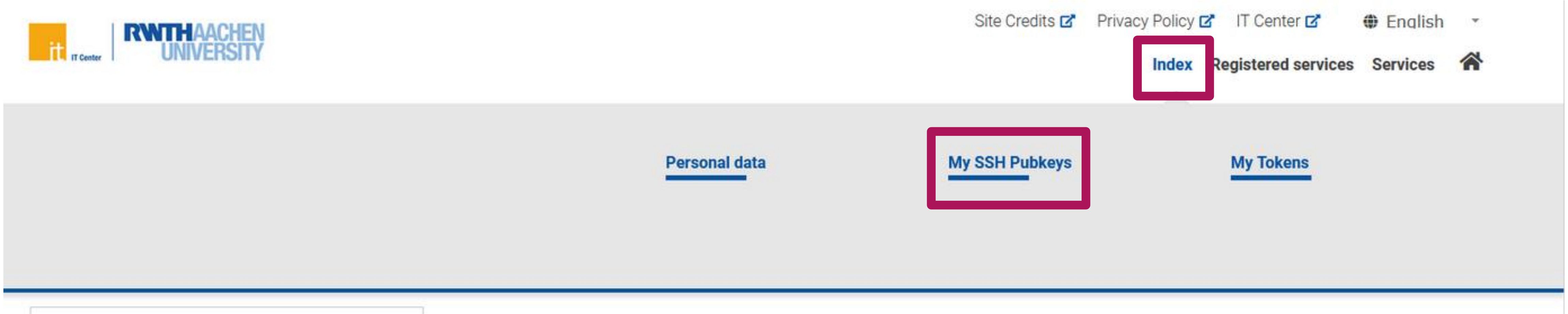
Type of key to generate:

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

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

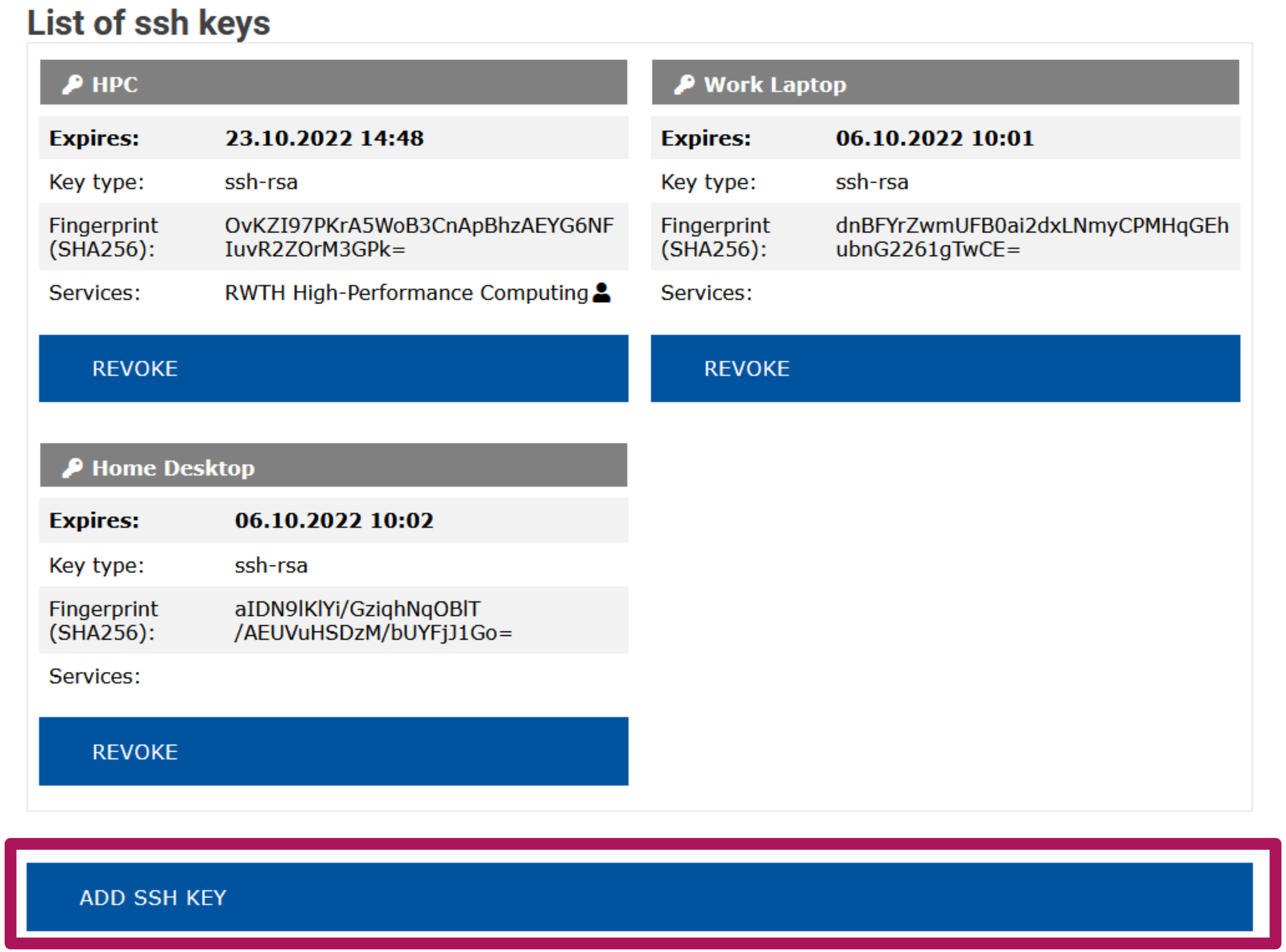
3. Upload a public SSH key

- 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):	OvKZI97PKrA5WoB3CnApBhzAEYG6NFIuvR2ZOrM3GPk=
Services:	RWTH High-Performance Computing 👤

Work Laptop

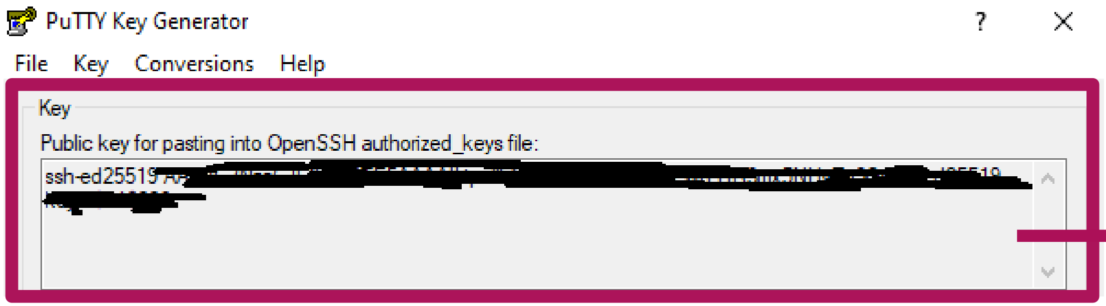
Expires:	**06.10.2022 10:01**
Key type:	ssh-rsa
Fingerprint (SHA256):	dnBFYrZwmUFB0ai2dxLNmyCPMHqGEhubnG2261gTwCE=
Services:	

Home Desktop

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

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:
  - 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

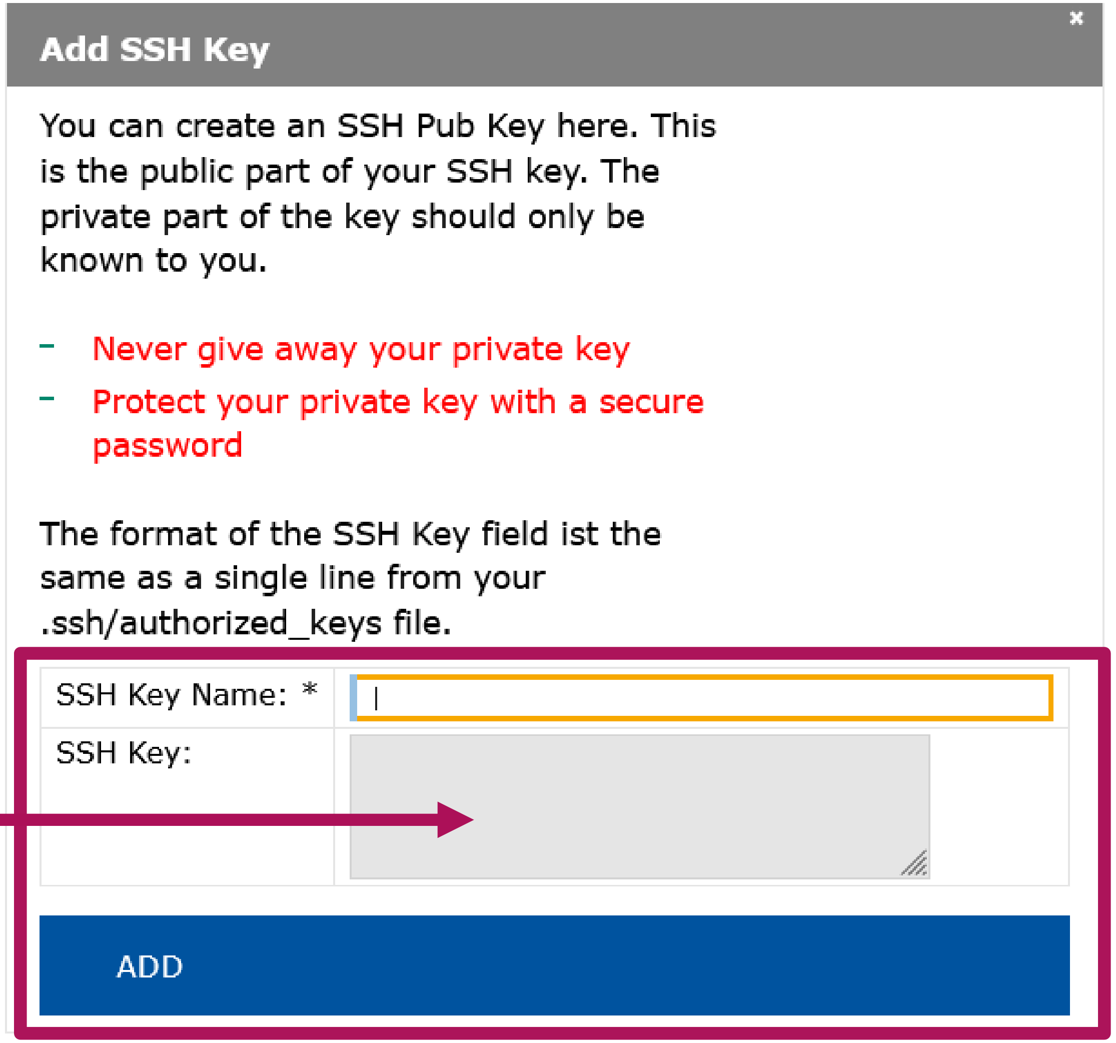


Key

Public key for pasting into OpenSSH authorized_keys file:

ssh-ed25519 [redacted]

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


Add SSH 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

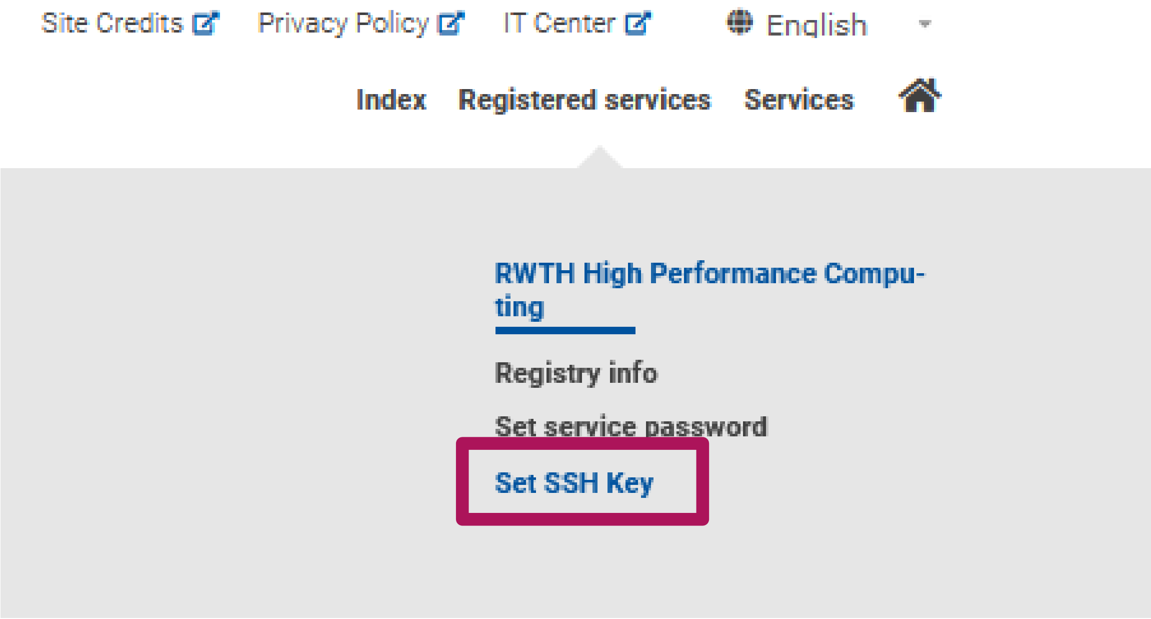
The format of the SSH Key field ist the same as a single line from your .ssh/authorized_keys file.

SSH Key Name: *

SSH Key:

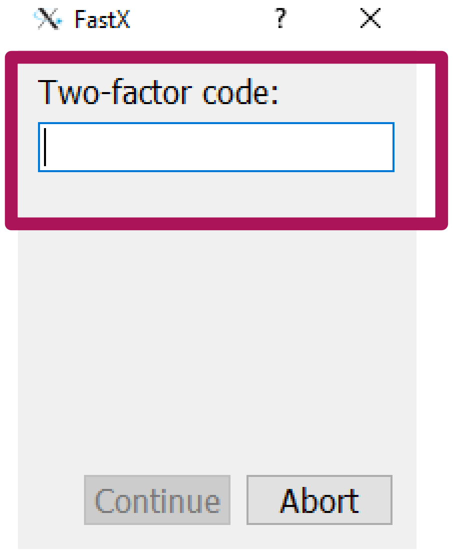
4. Assign SSH Key to Service HPC

- 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



5. Log In to a MFA Node

- Only one MFA node at the moment: `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



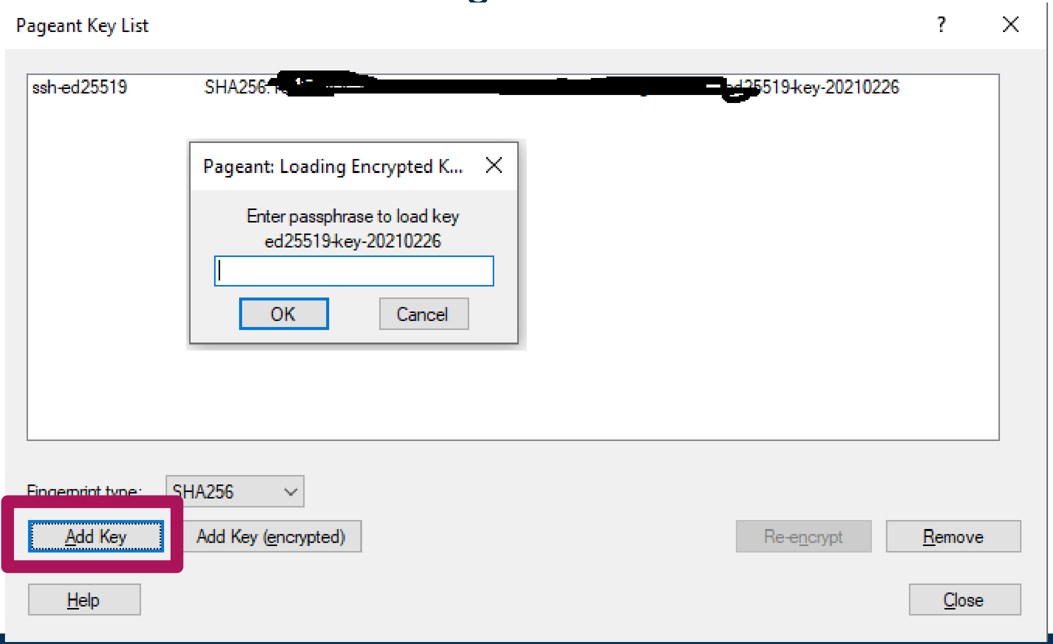
Two-factor code:

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



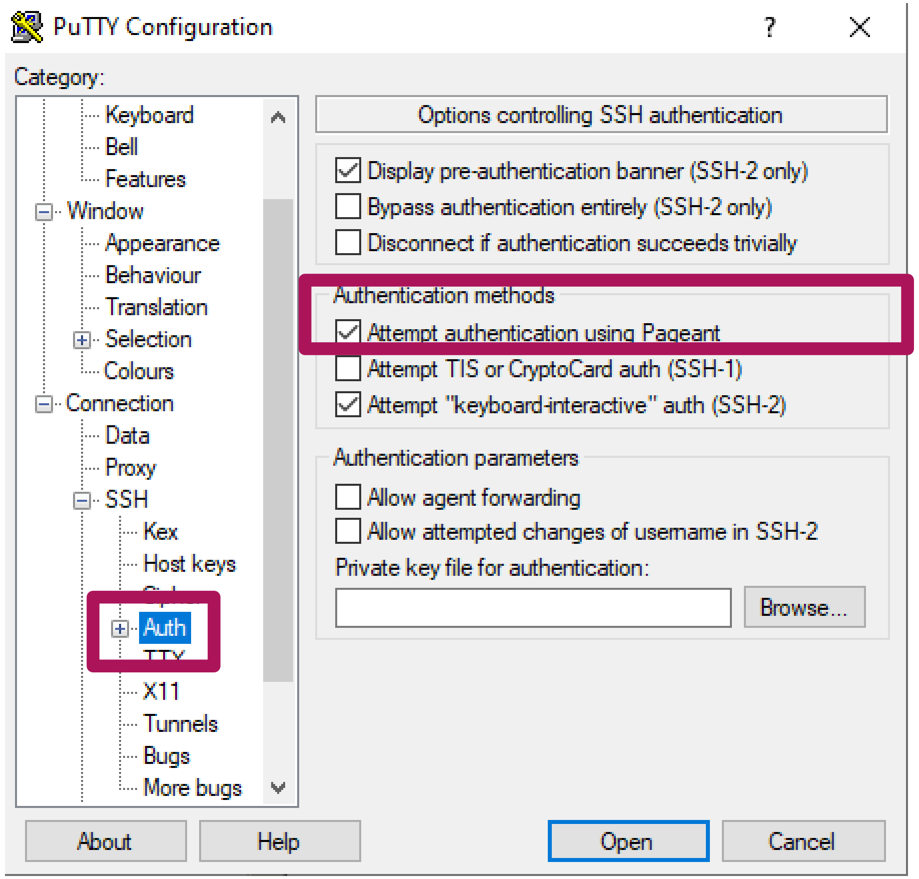
Pageant Key List

ssh-ed25519 SHA256:[redacted]d25519-key-20210226

Pageant: Loading Encrypted K...

Enter passphrase to load key ed25519-key-20210226

Fingerprint type: SHA256



PuTTY Configuration

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 can help to secure your personal and research data
- Workflows might change a bit
- MFA might be mandatory in future, use the opportunity to test NOW
- Feedback is welcome: servicedesk@itc.rwth-aachen.de
- IMPORTANT: Pilot phase at the moment, no additional security for now (since you can still login on nodes without MFA)

Questions?