technische universität
dortmund

LiDO3

User account application

IT & Medien Centrum | CC HPC

November 16, 2023

Table Of Contents

Chapter 1

LiDO3 - User account application

1.1 Scope

This document intends to guide you through the first steps needed for user account application for LiDO3, TU Dortmund's high performance cluster (HPC): to get access to the system.

We renounce the explicit mention of the female form and hope that this omission allows fluent reading of the instructions.

1.2 Non-scope

Starting jobs, programming, especially parallel programming and the usage of libraries like MPI[1] is not subject of this document. Neither is it a guide for structuring workload to scale on a HPC environment.

[1] https://en.wikipedia.org/wiki/Message_Passing_Interface

Chapter 2

Prerequisites

2.1 How do I get / extend a user account?

2.1.1 Application

Applications can be submitted by students and permanent employees of the *Technische Universität Dortmund*.

In most cases, students and employees of the *Technische Universität Dortmund* can use the LiDO3 usermanagement portal[1] to submit an application online.

In this application form, it is mandatory to provide information about the intended purpose of LiDO usage, termination date of LiDO usage, email address of your approver (your supervising professor) and your public SSH key which you are supposed to have generated before submitting the form.

For generating your public and private key pair see page 6.

To minimize the attack surface for cyber attacks, the LiDO3 usermanagement portal is reachable from within the TU Dortmund University network only, i.e. your client machine must have an IP address assigned in the range between 129.217.0.1 and 129.217.255.255; if you connect from outside the university or are connected via Wifi network `eduroam`, first establish a VPN connection to `vpn.tu-dortmund.de`; single-sign-on login with uni account is mandatory).

[1] https://l3umw.lido.tu-dortmund.de:8193/usermanagement/static/lido3-account-application-form.html

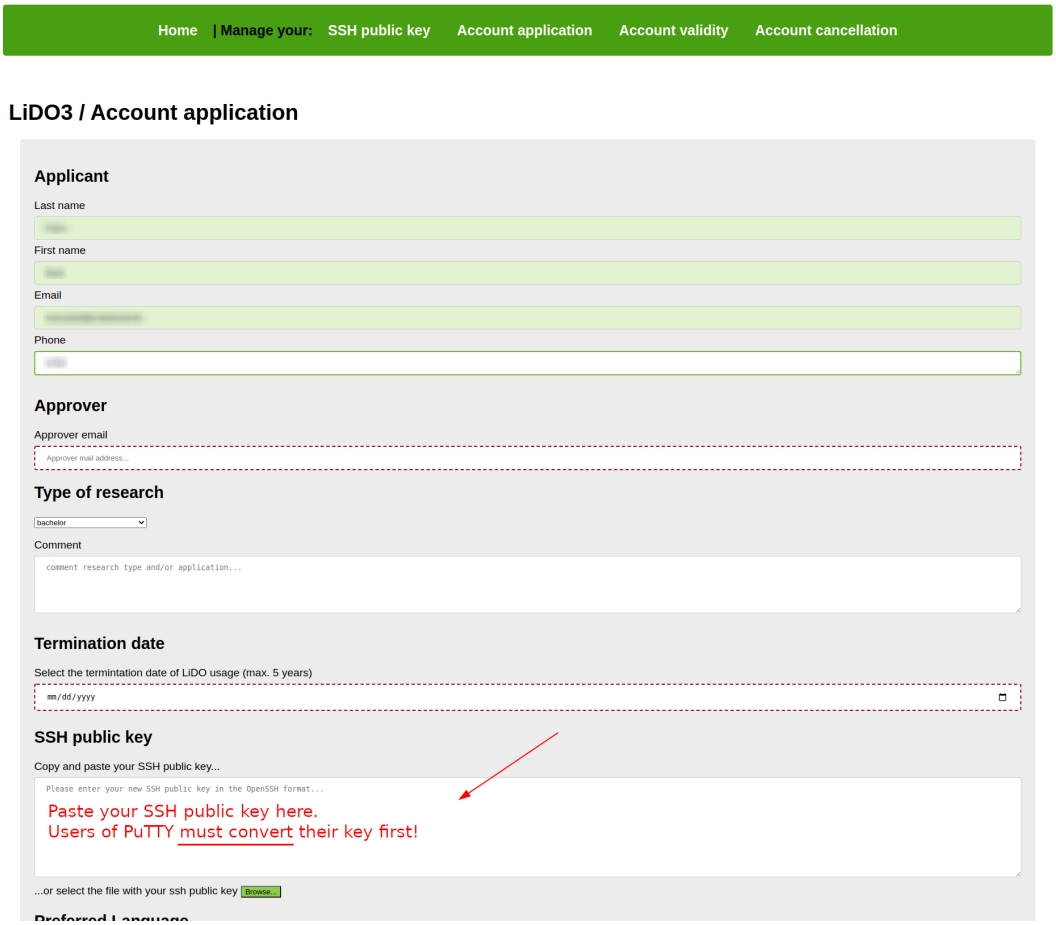

Figure 2.1: Insert your generated public key into the *"SSH Public Key"* field to submit your public key.

Users of the PuTTY client must convert their key into the OpenSSH format first, see figure 2.4 on page 11.

To manage your existing LiDO3 user account, please use the web forms in the LiDO3 user management portal[2]To minimize the attack surface for cyber attacks, the LiDO3 usermanagement portal is reachable from within the TU Dortmund University network only, i.e. your client machine must have an IP address assigned in the range between 129.217.0.1 and 129.217.255.255; if you connect

[2] https://l3umw.lido.tu-dortmund.de:8193/usermanagement/static/index.html

from outside the university or are connected via Wifi network `eduroam`, first establish a VPN connection to `vpn.tu-dortmund.de`; single-sign-on login with uni account is mandatory).

If the project is funded by the *Fachhochschule Dortmund* or *UA Ruhr* within the framework of a cooperaton with the *Technische Universität Dortmund*, you have to open a ticket at the Service Desk[3]. Please note that this application can only be used by professors for their own projects, doctoral or post-doctoral research.

2.1.2 Approval

Upon submitting the application form[4], your approver (your supervising professor) will be informed via e-mail about your account application. The approver is kindly requested to accept or decline your application. Once the approver has accepted or declined your LiDO3 account application, a ticket is generated in the ITMC ticket system that involves informing the LiDO team. If the approver does not react, a reminder will be sent every Monday after 7 days. If the approver still does not react, the LiDO team will notify you about the delay.

2.1.3 Account creation

Once an approver has accepted your account application, the LiDO team gets informed by the ticket system about it. Typically, within a work day or two your account is then semi-automatically created. If it takes considerably longer and you do not get any feedback about your account creation, it is almost certain the LiDO team has not yet been informed about your pending account application, but that the approver has overlooked the e-mail that asks for approval or denial of your account application. In that case, you may want to check with your approver first before contacting the *Service Desk*.

2.2 SSH Key

SSH keys are used to identify yourself to a computer using public key cryptography[5] instead of a password. On one hand, this is done for security reasons – a SSH key is much harder to crack than a password, if at all feasible within reasonable time – and on the other hand for user comfort.

[3] https://itmc.tu-dortmund.de/das-itmc/kontakt/service-desk/
[4] https://l3umw.lido.tu-dortmund.de:8193/usermanagement/static/lido3-account-application-form.html
[5] https://en.wikipedia.org/wiki/Public-key_cryptography

The use of SSH keys is mandatory. You **cannot** log into LiDO3 with a username and password. In case you are prompted for a password other than your SSH key passphrase when you try to log in to either one of the gateway servers, something is entirely wrong:

- You are using a SSH client that does only support authentication via passwords, but maybe not via SSH keys. Or
- You used the SSH public key in your client instead of the SSH private key. Or
- The SSH public key entered in the LiDO3 account application web form (see 2.1) got scrambled (or its PuTTY file format representation was used instead of the canonical OpenSSH file format) such that your valid SSH private key does not match the scrambled SSH public key stored on LiDO3 any more, or
- The SSH private key you are using to connect to LiDO3 belongs to a SSH public key not stored (any more?) on LiDO3.

The internet is full of good tutorials that show *how to create and use a SSH key*. The approach is a bit different for Linux users[6] and for Windows/PuTTY users[7]. We will, hence, keep our tutorial short:

2.2.1 Create SSH key pair on Unix

Open a shell and enter

```
$ ssh-keygen -t rsa -b 4096 -C "comment helping you identify this key"
```

or

```
$ ssh-keygen -t ed25519 -C "comment helping you identify this key"
```

If you already have other SSH key pairs, you can change the default filename in the following, otherwise just confirm the default by pressing the enter key.

[6] https://www.digitalocean.com/community/tutorials/how-to-set-up-ssh-keys--2

[7] https://www.howtoforge.com/how-to-configure-ssh-keys-authentication-with-putty-and-linux-server-in-5-quick-steps

```
Generating public/private rsa key pair.
Enter file in which to save the key
 (/home/<username>/.ssh/id_rsa):
```

When prompted, type a secure passphrase to protect[8] your SSH private key.

```
Enter passphrase (empty for no passphrase):
 [Type a passphrase]
Enter same passphrase again:
 [Type passphrase again]
Your identification has been saved in /home/<username>/.ssh/id_rsa.
Your public key has been saved in /home/<username>/.ssh/id_rsa.pub.
(...)
```

Copy and paste **only the SSH public key** into the user application form (see page 5) after the successful creation. Typically, the file containing the SSH public key is stored upon creation on your local system in a file with `.pub` file extension. Make sure to use the **SSH private key** when establishing a connection to the LiDO3 gateways with your SSH client software.

2.2.2 Create SSH key pair on Windows

2.2.2.1 OpenSSH client

With Windows Server 2022, Windows Server 2019, Windows 10 (build 1809 and later)[9] or newer) or Windows 11, an OpenSSH port is available in the command line prompt (in German-localized versions of Windows named 'Eingabeaufforderung'). This includes the program `ssh-keygen` described in the previous section 2.2.1. Its syntax is exactly the same. It will produce an SSH key pair in OpenSSH key format.

2.2.2.2 PuTTY client (and derived software clients)

If you want to rely on a GUI-based solution, you can use the PuTTY Key Generator (`puttygen.exe`) from the PuTTY Software Suite.[10][11]

[8] If someone ever gains access to your computer (or to the files stored there, e.g. by accessing your backup drives), they also gain access to **every** system that uses your SSH key pair. To add an extra layer of security, you **should** use a passphrase to encrypt your SSH private key.

[9] You can check the version of Windows 10 by pressing `Win-key+R` and then invoke the command `winver`. An information dialog will pop up detailing the specific version of your Windows 10 installation, e.g. `Version 21H1 (Build 19043.2251)`.

[10] https://www.chiark.greenend.org.uk/~sgtatham/putty/

[11] The MobaXterm SSH Key Generator is a direct clone of PuTTY Key Generator.

To create your SSH key pair for use on LiDO3 select either one of the four SSH key types “RSA”, “DSA”, “ECDSA”, “ED25519”. Please **do not use “SSH-1 (RSA)”**; the algorithm for this SSH key type is outdated and not supported any more on LiDO3 for security reasons.

To start the SSH key pair creation click on the button *Generate*.

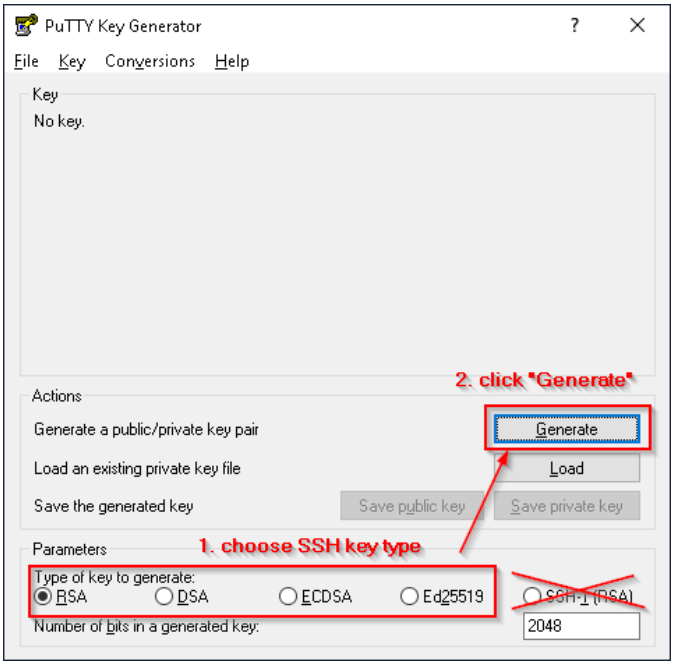

Figure 2.2: Choose SSH key type and click *Generate*.

For increased randomness in the generated SSH key, the user is required to move his mouse in random directions while the key is being generated. If you do not move your mouse around, the key generation will stall.

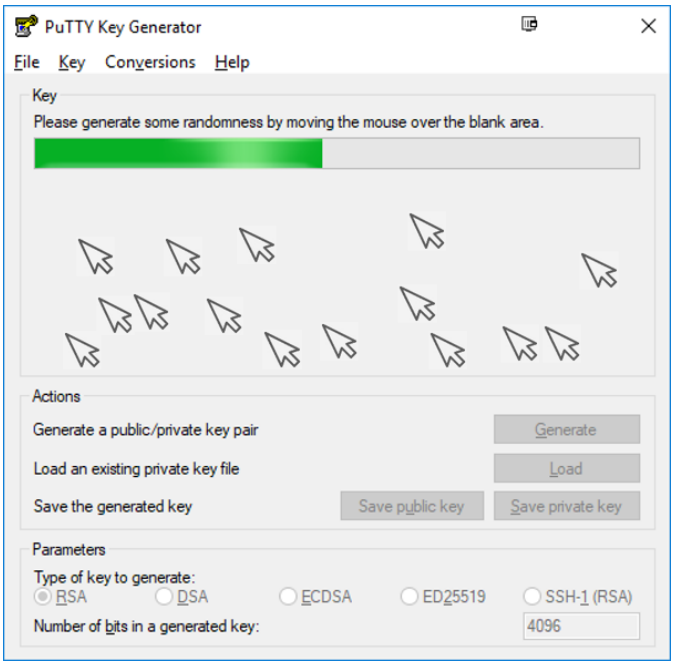

Figure 2.3: Random movements of the mouse pointer are used in order to create the key pair.

Once the SSH key pair has been generated, two steps remain: Firstly, store the SSH public key in a key file format that is understood by the OpenSSH server on LiDO3. Secondly, protect the SSH private key with a robust passphrase against abuse.

By default, PuTTY uses, unfortunately, its own propriatory key file formats, both for the SSH private key and the SSH public key. Hitting the button `Save public key` would store the SSH public key in PuTTY's propriatory key file format. For convenience, though, the SSH public key is also shown in OpenSSH key file format in the top section of the PuTTY Key Generator's main window, once it has been generated. Copy your freshly created SSH public key from the frame labeled `Public key for pasting into OpenSSH authorized_keys file` (see figure 2.4) and paste it into the LiDO3 account application web form (see figure 2.1 on page 5).

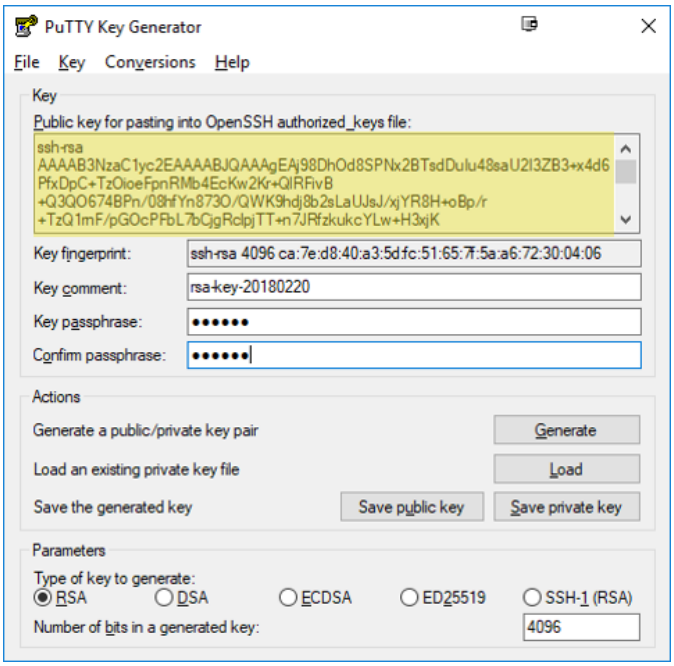

Figure 2.4: Save the SSH private key and the SSH public key. Copy and paste the SSH public key (marked in yellow) to the user application form.

A typical, valid SSH public keys (in OpenSSH key file format) starts with either one of the following strings. Please make sure you do not try to upload the SSH public key in PuTTY's key file format:

```
ssh-rsa AAAAB3NzaC1[...]
ssh-dss AAAAB3NzaC1[...]
ssh-ed25519 AAAAC3N[...]
```

The last step is to enter a passphrase which is later used to protect your SSH private key in the text field labeled `Key passphrase` and then hit the button `Save private key`. Select a directory to your liking to save the SSH private key and make sure nobody else has access to this directory. You will require this file in the future every time you intend to connect to the LiDO3 gateways.

If you intend to use your SSH private key with programs other than PuTTY, programs that use the OpenSSH key file format, e.g. with ThinLinc (see section **??**), you are advised to save a copy of your SSH private key in OpenSSH key file format right away. Convert it via menu `Conversions`→`Export OpenSSH key` to a new file. (The conversion can be done at a later time by first loading your SSH private key in PuTTY key file format (file extension `*.ppk`) as well.)

2.2.3 Changing your SSH public key

Unlike on other Unix systems your SSH key will not be visible in `~/.ssh/authorized_keys` on LiDO3. Thus any changes to your key must be advertised in the LiDO3 user management portal[12].To minimize the attack surface for cyber attacks, the LiDO3 usermanagement portal is reachable from within the TU Dortmund University network only, i.e. your client machine must have an IP address assigned in the range between 129.217.0.1 and 129.217.255.255; if you connect from outside the university or are connected via Wifi network `eduroam`, first establish a VPN connection to `vpn.tu-dortmund.de`; single-sign-on login with uni account is mandatory).

[12] https://l3umw.lido.tu-dortmund.de:8193/usermanagement/static/index.html

2.2.4 Picture credits

- Windows Logo - Wiki Commons[13]
- Apple Logo - Wiki Commons[14]
- Tux Logo - Wiki Commons[15]
- Computer shape - Openclipart[16]
- Server shape Openclipart[17]
- Light bulb - Openclipart[18]
- Warning triangle - Openclipart[19]
- Clock - Openclipart[20]
- TU Dortmund math tower - tu-dortmund.de[21]
- Remaining screeshots and figures - created by the LiDO Team

[13] http://commons.wikimedia.org/wiki/Category:Microsoft_Windows_logos
[14] http://commons.wikimedia.org/wiki/File:Apple_logo_black.svg?uselang=de
[15] http://commons.wikimedia.org/wiki/Tux#/media/File:Tux.svg
[16] https://openclipart.org/detail/17391/computer
[17] https://openclipart.org/detail/171414/router
[18] https://openclipart.org/detail/211389/lightbulb
[19] https://openclipart.org/detail/14428/h0us3s-Signs-Hazard-Warning-9-by-h0us3s
[20] https://openclipart.org/detail/217065/3-oclock
[21] http://www.tu-dortmund.de/Bilder/Bilderpool2013/content/TU_Dortmund_Campus1_large.html