Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Services
Direction

ETH Zurich
Binzmuehlestrasse 130
8092 Zurich

www.id.ethz.ch

How to create an SSH key pair

The SSH key pair is used to log in to LeoMed via the command line.

- the ed25519 algorithm for generating the SSH key pair is mandatory
- the passphrase (non-empty, of minimum 16 characters) protection of the SSH key pair is mandatory
- format convention for sharing the public SSH key: as file named <username>.pub

Linux / Unix (macOS)

1	**a.** Open your terminal application of choice **b.** Generate the SSH key using the following command. [user@workstation]$ ssh-keygen -t ed25519
2	**a.** Fill in the required information **b.** Introduce a **strong** *passphrase* Important It is mandatory to encrypt the key with a strong passphrase with at least 16 characters.

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Services
Direction

ETH Zurich
Binzmuehlestrasse 130
8092 Zurich

www.id.ethz.ch

3	Example [user@workstation]$ ssh-keygen -t ed25519 Generating public/private ed25519 key pair. Enter file in which to save the key (/home/<username>/.ssh/id_ed25519): Enter passphrase (empty for no passphrase): ********** Enter same passphrase again: ********** Your identification has been saved in /home/<username>/.ssh/id_ed25519 Your public key has been saved in /home/<username>/.ssh/id_ed25519.pub The key fingerprint is: SHA256:LhpfwohLVJM2h2N/q4UHIJNxzUysZ8pD2J1isJ91sBg bmx@LAPTOP-GHKPS84N The key's randomart image is: +--[ED25519 256]--+ | . .*. | | .+Eo* | | +=@=.+ | | o*BBB . | | .= Bo.S | | . .*o = . | | o o.= * | | . . + B | | . . o | +----[SHA256]-----+
4	Copy the **public** key and rename it to *<username>.pub* (where <username> should be replaced by your ETH user name). The following command will copy the public key in the right format to your Desktop (assuming that the key was saved to */home/<username>/.ssh/id_ed25519;* see the output above): [user@workstation]$ ~/.ssh/id_ed25519.pub ~/Desktop/<username>.pub

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Services
Direction

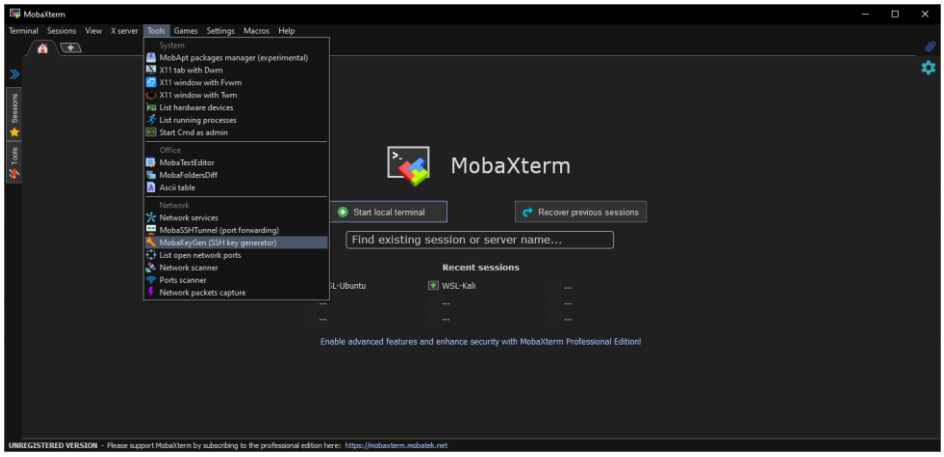
ETH Zurich
Binzmuehlestrasse 130
8092 Zurich

www.id.ethz.ch

Windows

Important

Windows 10 includes a built-in OpenSSH client since the April 2018 update, however, we will use MobaXterm for compatibility reasons.

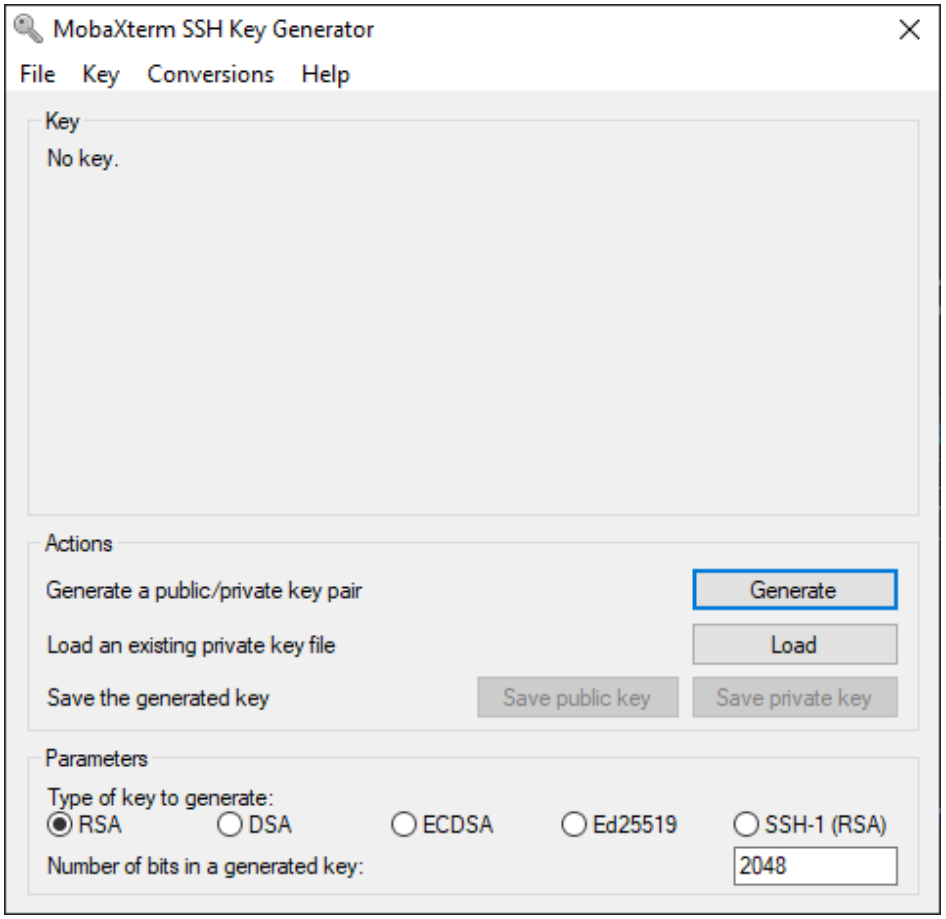
1	**a.** Open mobaXterm **b.** Open the *Tools* menu **c.** Clink *MobaKeyGen (SSH key generator)*	

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Services
Direction

ETH Zurich
Binzmuehlestrasse 130
8092 Zurich

www.id.ethz.ch

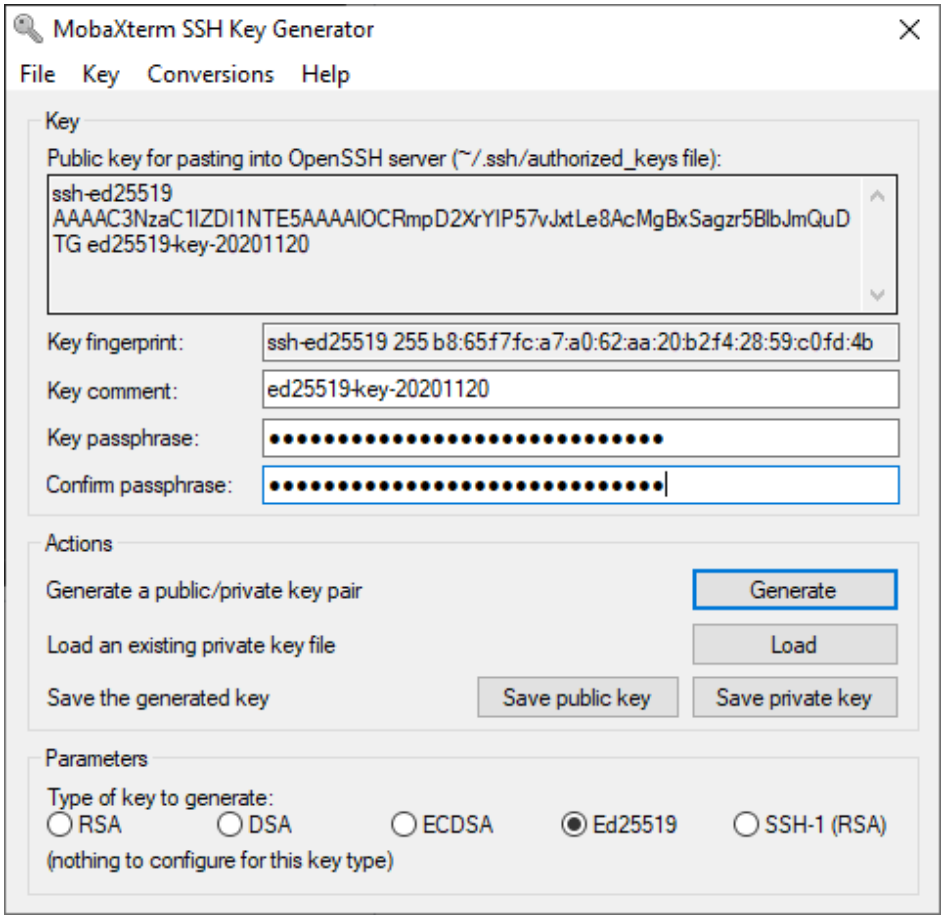
2	**a.** Select the type *Ed25519* **b.** Click *Generate* ***c.*** *Introduce a* ***strong*** *passphrase* Important It is mandatory to encrypt the key with a strong passphrase with at least 16 characters.	

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Services
Direction

ETH Zurich
Binzmuehlestrasse 130
8092 Zurich

www.id.ethz.ch

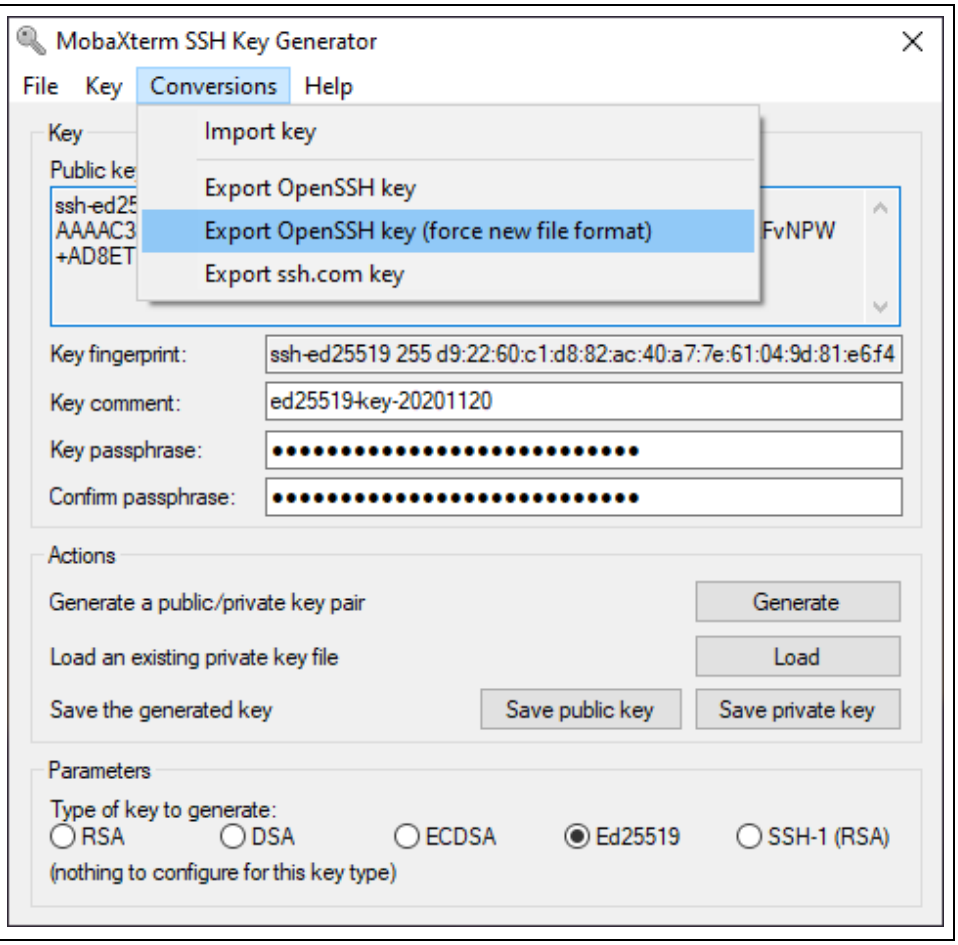


Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Services
Direction

ETH Zurich
Binzmuehlestrasse 130
8092 Zurich

www.id.ethz.ch

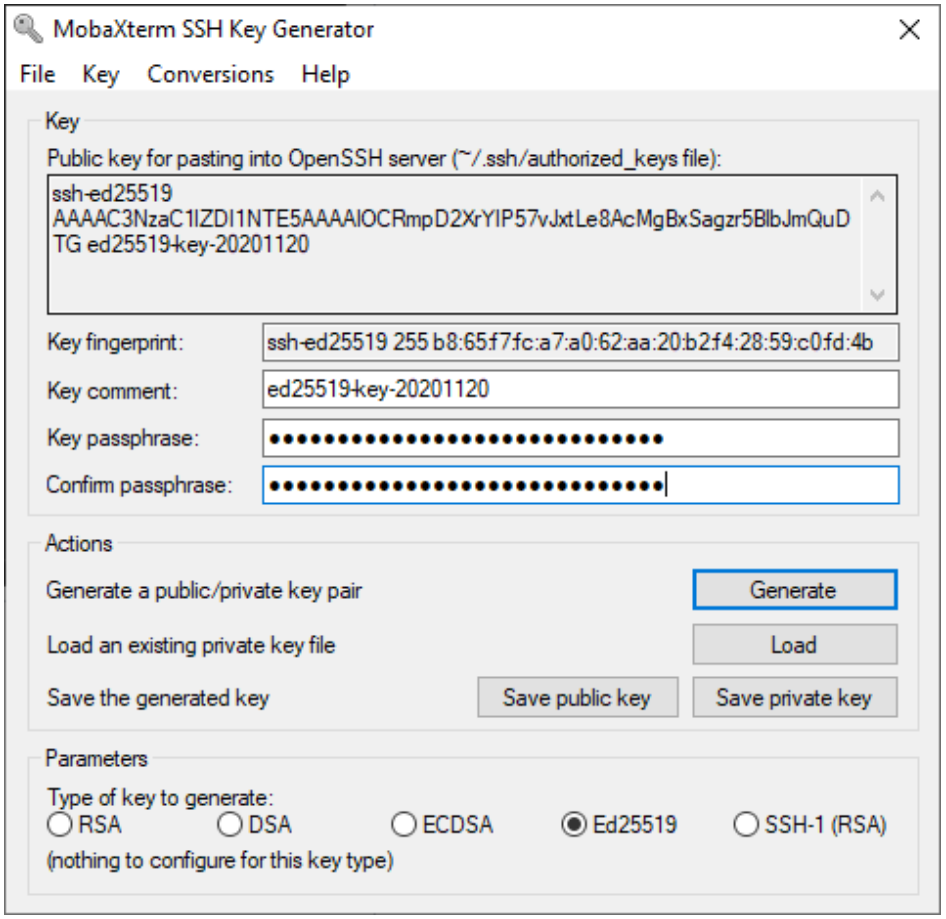
3	Save the *Private key* **a.** Open the *Conversions* menu **b.** Select *Export OpenSSH key (force new file format)*	

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Services
Direction

ETH Zurich
Binzmuehlestrasse 130
8092 Zurich

www.id.ethz.ch

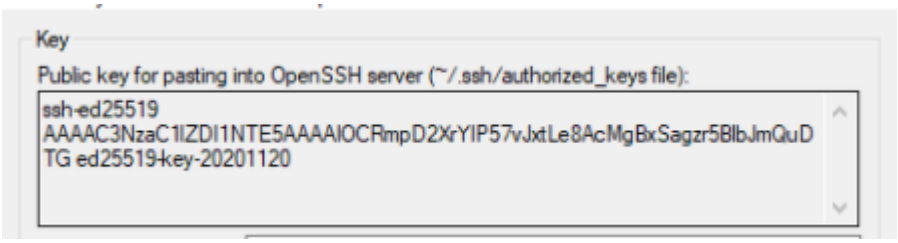
4	Save the *Public key* by clicking the *Save public key* button	

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Services
Direction

ETH Zurich
Binzmuehlestrasse 130
8092 Zurich

www.id.ethz.ch

5	Open the *Public key* file you just saved with a text Editor (such as *Notepad)* and overwrite it **only** with the content from the box and save it. This is because the format used by Putty/MobaXterm for the public key is not the expected one	

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Services
Direction

ETH Zurich
Binzmuehlestrasse 130
8092 Zurich

www.id.ethz.ch

How to create a GPG key pair

This document guides you through the steps of creating a GPG key. A new GPG key pair should be created for LeoMed. This pair should only be used for LeoMed.

The GPG key pair is used to encrypt a QR code needed for generating the second factor. This encrypted code will be sent to you via email. You will be able to decrypt this file with your private GPG key.

- the ed25519 algorithm for generating GPG key-pairs is recommended
- the passphrase (non-empty, of minimum 16 characters) protection of the GPG key-pair is recommended
- format convention for sharing the public GPG key: as file named <username>.gpg

Terminal

To execute commands in the terminal

1. open your terminal application
2. type or paste the command into the terminal window
3. hit enter

Example:

[user@workstation]$ ls

1. open your terminal application
2. type "ls" into the terminal window (*[user@workstation]$* indicates the machine you are currently working on and might look different depending on your settings)
3. hit enter

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Services
Direction

ETH Zurich
Binzmuehlestrasse 130
8092 Zurich

www.id.ethz.ch

Linux / Unix (macOS)

1	**Install the GPG software** using these terminal commands **a.** Linux [user@workstation]$ sudo apt-get install gnupg2 **b.** macOS After installing homebrew, you can use the `brew` command to install GPG [user@workstation]$ brew install gpg	
2	**a.** Open your terminal application of choice **b.** Generate the GPG key using the following command. [user@workstation]$ gpg --gen-key	
3	Fill in the required information including your real name and your work email Important Please avoid the use of special characters like umlauts	

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Services
Direction

ETH Zurich
Binzmuehlestrasse 130
8092 Zurich

www.id.ethz.ch

4

Example

```
[user@workstation]$  gpg --gen-key
gpg (GnuPG) 2.2.19; Copyright (C) 2019 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: John Smith
Email address: john.smith@email.corp
You selected this USER-ID:
    "John Smith <john.smith@email.corp>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: key 94F3B324F9CA5741 marked as ultimately trusted
gpg: revocation certificate stored as '/home/<username>/.gnupg/openpgp-
revocs.d/21AF418DC988D4B85B81C05894F3B324F9CA5741.rev'
public and secret key created and signed.

pub   rsa3072 2020-11-20 [SC] [expires: 2022-11-20]
      21AF418DC988D4B85B81C05894F3B324F9CA5741
uid                    John Smith <john.smith@email.corp>
sub   rsa3072 2020-11-20 [E] [expires: 2022-11-20]
```

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Services
Direction

ETH Zurich
Binzmuehlestrasse 130
8092 Zurich

www.id.ethz.ch

5	**Export public key** To export the public key into a file (for instance, on your Desktop), run the following command: [user@workstation]$ gpg -a --output ~/Desktop/<username>.gpg --export <key_ID> • <username> should be replaced by your LeoMed username • <key_ID> should be replaced by the GPG key's ID (in the above example, "21AF418DC988D4B85B81C05894F3B324F9CA5741"; the `gpg --list-key` command can also be used to retrieve the key ID.)

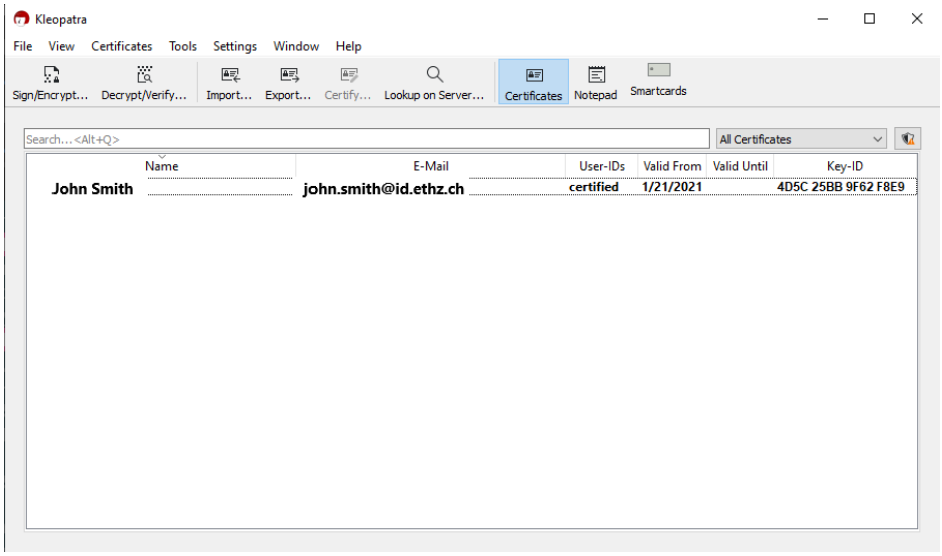
Windows

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Services
Direction

ETH Zurich
Binzmuehlestrasse 130
8092 Zurich

www.id.ethz.ch

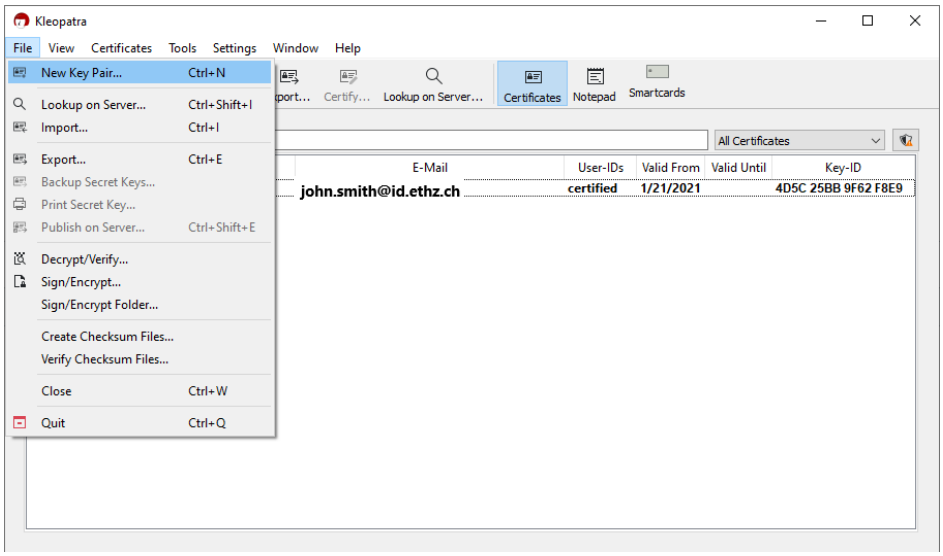
1	**a.** Install GPG4Win (also known as Kleopatra) **b.** Open Kleopatra **c.** Create a new GPG key pair **d.** Select Create a personal OpenGPG key pair	**b.** Kleopatra UI  **c.** Create a new GPG key pair

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

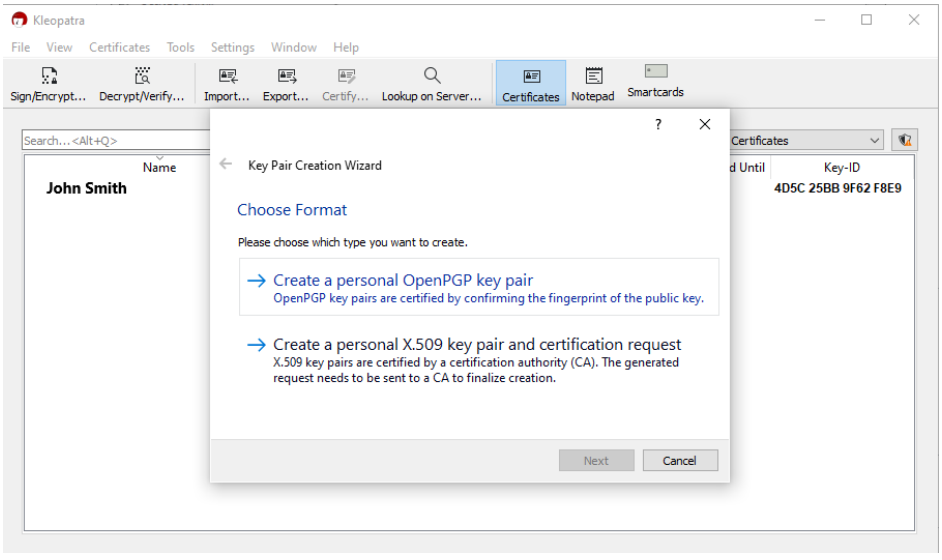
IT Services
Direction

ETH Zurich
Binzmuehlestrasse 130
8092 Zurich

www.id.ethz.ch



d. Key Pair creation

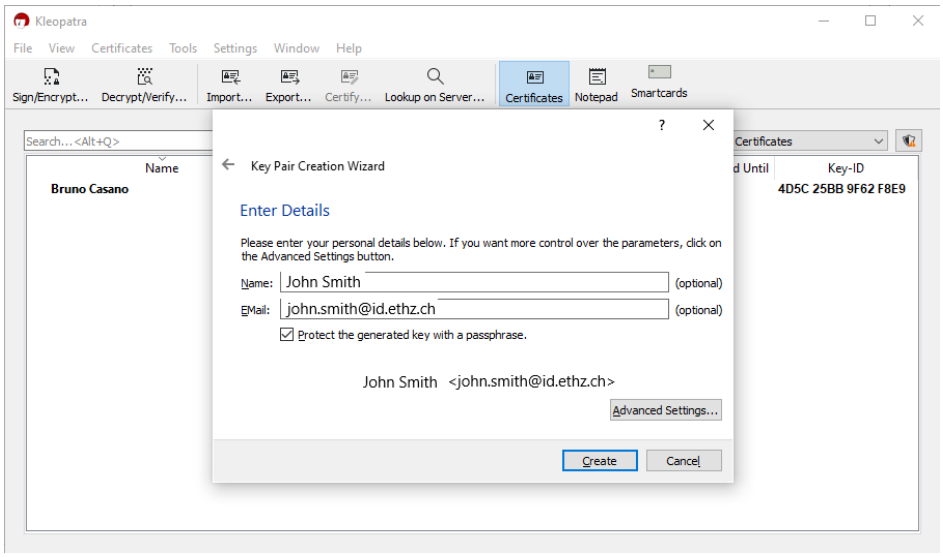
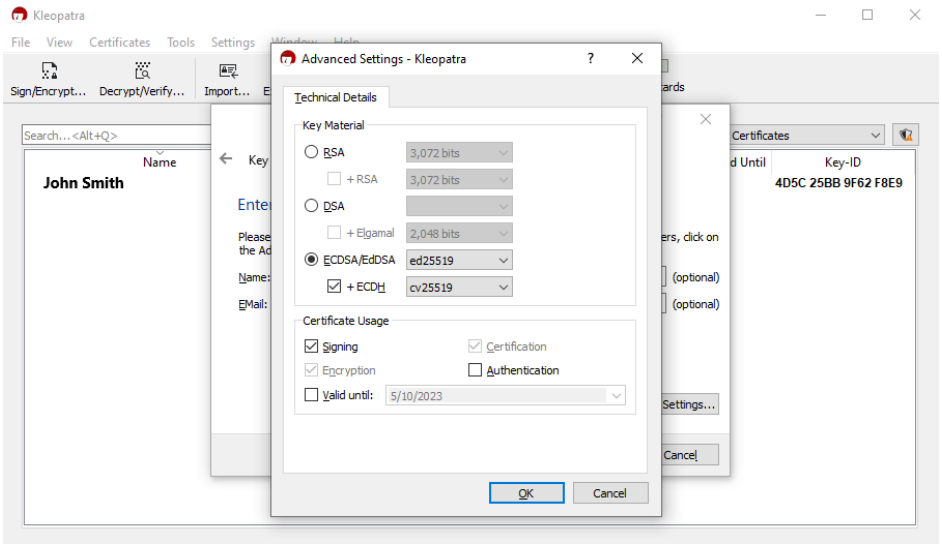


Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Services
Direction

ETH Zurich
Binzmuehlestrasse 130
8092 Zurich

www.id.ethz.ch

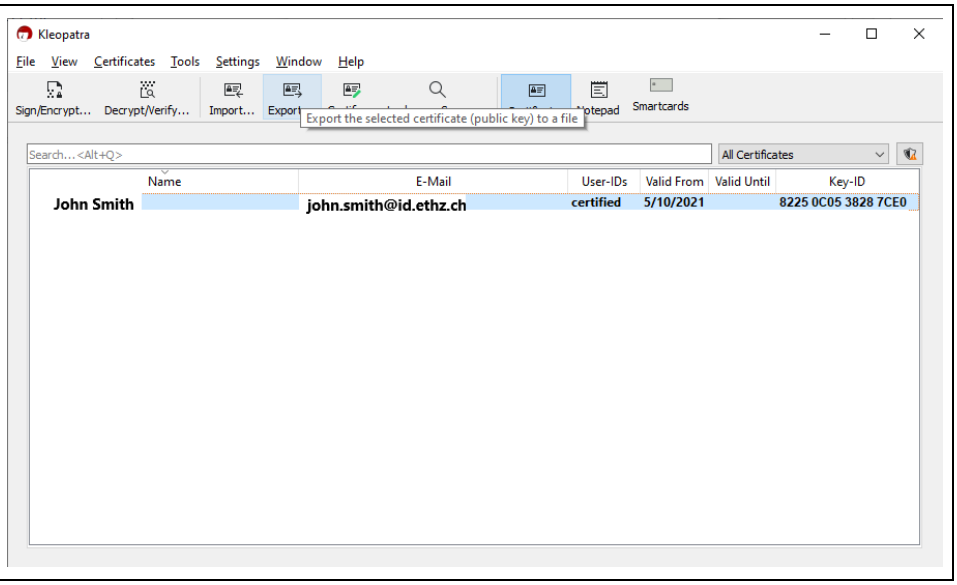
2	**a.** Fill in the required information including your real name and your work email **b.** Make sure you protect the pair with a passphrase by checking the *Protect the generated key with a passphrase* checkbox. **c.** Click the *Advanced Settings* button and update the *Key Material* to ECDSA/EdDSA and un-select the *Valid until* checkbox, as shown in the screenshot Important Please avoid the use of special characters like umlaut	 

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Services
Direction

ETH Zurich
Binzmuehlestrasse 130
8092 Zurich

www.id.ethz.ch

3	Export public key to a file	

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IT Services
Direction

ETH Zurich
Binzmuehlestrasse 130
8092 Zurich

www.id.ethz.ch

How to assemble the required information in the correct format

1. Make sure your public GPG key file is called *<username>.gpg,* where <username> is to be replaced by your LeoMed user name.
2. Make sure your public SSH key file is called *<username>.pub. O*nly required if you request command-line access to LeoMed.
3. Prepare a text file named *<username>.addr* containing your work-related contact information.

Dos and don'ts

These are some examples of the things we expect from the `.addr` file, and some things we don't support.

- Avoid the use of umlaut or special characters
- Avoid the use of "field: value" format, i.e., Name: Andrea Mueller

Good

```
Andrea Mueller
Zuerich
andrea.mueller@foo.ethz.ch
```

Bad

```
Andrea Müller
Zürich
email: andrea.mueller@foo.ethz.ch
```