

SSH Key

- [Generating a SSH key on Linux](#)
- [Generating a SSH Key in a Windows](#)
 - [Converting SSH Keys to PPK Format](#)

Generating a SSH key on Linux

Run following commands with properly defining your email in a comment:

```
ssh-keygen -t ed25519 -f ~/.ssh/id_ed25519 -C "john@example.com"  
cat ~/.ssh/id_ed25519.pub
```

Here we explain used options:

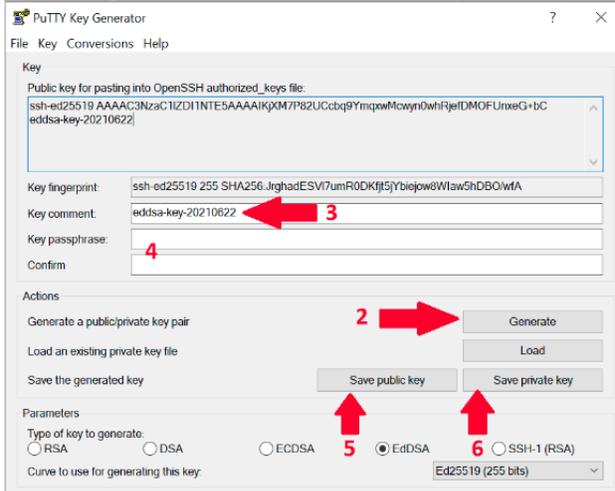
- -t: Specifies the type of key to create, we recommend most secure option currently - Ed25519
- -f: Specify the filename of the generated key file. If you want it to be discovered automatically by the SSH agent, it must be stored in the default `~/.ssh` directory within your home directory.
- -C: An option to specify a comment. It's purely informational and can be anything. But it's usually filled with <login>@<hostname> who generated the key.

Then copy output of cat command and use it in desired application like TDS Portal profile, Gitlab profile, etc...

Generating a SSH Key in a Windows

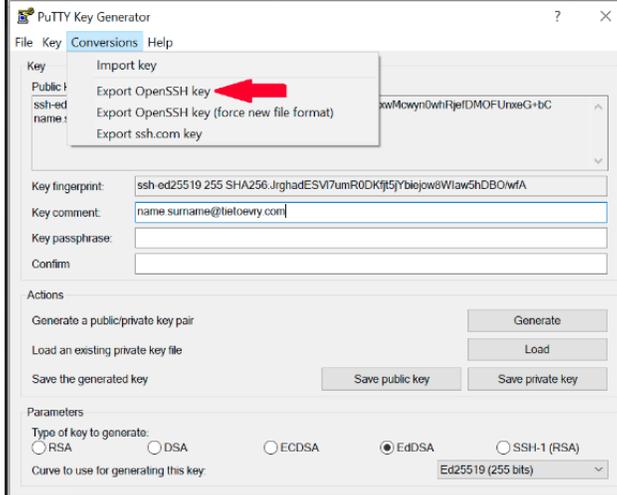
Download [PuTTY Key Generator](#) (puttygen.exe) from official Putty home page <https://www.putty.org/> and start it.

1. Change type to EdDSA, default 256bits is fine. We recommend using EdDSA as it is more secure than RSA, [RSA causes slower connection as it has bigger overhead](#) and long term future plans of SSH community are to get rid of RSA.
2. Run the program and click on **Generate** and move your mouse (within the SSH generator window) until key is generated

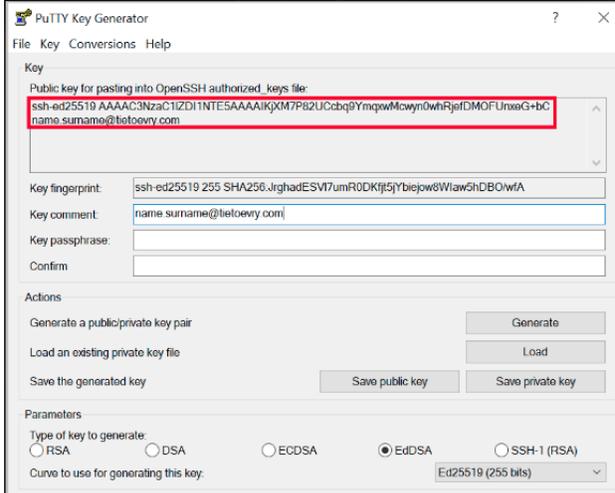


3. Change *Key comment* to your email address in format like in this example name.surname@tietoevry.com
4. Optional: fill *Key passphrase* and confirm passphrase if you need one.
If you skip this step then you need to confirm that you want to save the keys without passphrase in the next steps.
5. Save public key as **id_ed25519.pub**
6. Then save your private key in 2 commonly used formats. Please remember to keep private keys as private, never share it with anyone. Only public key can be shared.
 1. Putty format - Click Save private key and store as **id_ed25519.ppk**

2. OpenSSH format - From the top menu in Conversions select Export OpenSSH Key and save it as **id_ed25519**



7. Copy content of "Public key for pasting into OpenSSH authorized_keys file"



8. Go to the TDS Portal and click on user icon located in top right corner of portal page. Then click on your name.

9. In your profile click on "EDIT" button and then enter public part of your SSH key.

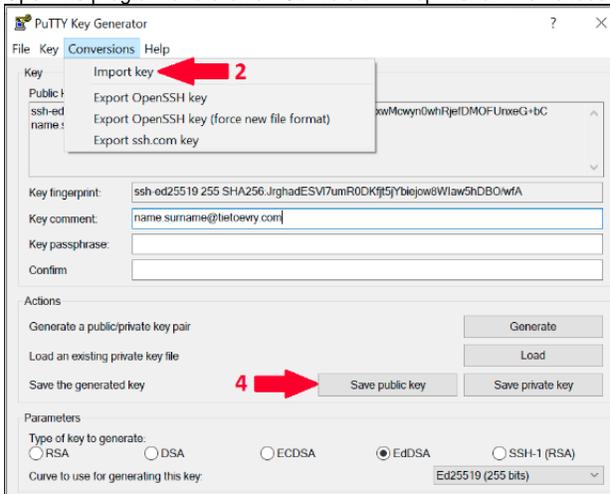
10. Paste copied key from the step 7. Click on the **Save** button.

11. Save all your generated SSH key files into folder `~/ssh` which is the same as `C:\Users\<your_username>\.ssh` folder. Thanks to this standardised location some of your applications will start using SSH key automatically. You will be always able to find it in case of need. Also TDS support team can help you more promptly in case of need.

Converting SSH Keys to PPK Format

1. [Download PuTTY Key Generator](#)

2. Open the program and click on *Conversion* in top menu. Then choose *Import key*.



3. Locate your key in your computer and click open.
4. Once the key is loaded, you can save it as PPK file by clicking on **Save Private Key** or on **Save Public Key** if you want public version of your key.