Linux Install Party Guide (1/2)

Dual Boot

- If the Windows installation is using BitLocker:
  - **Note down the BitLocker recovery key before installation** (just to be sure): https://aka.ms/myrecoverykey
  - If Windows and Linux share the same disk, **resize the partition on Windows** (Linux will refuse to do so)
  - You might need to partition the system manually, because some installers refuse to work if they detect a BitLocker encrypted Windows; in this case call for backup ;)
  - ***Alternatively, disable BitLocker in Windows (and optionally re-enable it later):* https://help.ubuntu.com/bitlocker**
- After installation:
  - Make sure the Windows installation has an entry in GRUB, if not append "`GRUB_DISABLE_OS_PROBER=false`" to `/etc/defaults/grub` and run "`sudo update-grub`"
  - Set Windows hardware clock to UTC: open `regedit.exe`, navigate to "`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\`" and create a key called "`RealTimeIsUniversal`" of type "`DWORD (32-bit) Value`" with value "`1`".

Eduroam

- Download root certificate from https://pki.pca.dfn.de/dfn-ca-global-g2/cgi-bin/pub/pki?cmd=getStaticPage;name=index;id=2&RA_ID=3770 (click on "Wurzelzertifikat")
- Connect to *eduroam* using the following settings:
  - WiFi-Security: "WPA & WPA2 Enterprise"
  - Authentication: "Protected EAP (PEAP)"
  - Anonymous Identity: "wlan@tu-berlin.de"
  - Domain: "tu-berlin.de"
  - CA certificate: select the one you downloaded
  - PEAP version: "Automatic"
  - Inner authentication: "MSCHAPv2"
  - Username: "<tub-username>@tu-berlin.de"
  - Password: "<tub-password>"

Link to the ZECM tutorial ***(includes link to certificate)***

Linux Install Party Guide (2/2)

TU VPN

- Package “`network-manager-openconnect-gnome`” required
- Settings → Network → VPN → “+” (Add VPN) → “Multi-protocol VPN client (openconnect)”
- In Identity:
  - VPN Protocol: “Cisco AnyConnect or OpenConnect”
  - Gateway: “vpn.tu-berlin.de”
  - **User Agent: “AnyConnect Linux_64 4.10.07061”**
- Keep everything else as is

SSH-Key

- You can create an SSH-key using “`ssh-keygen`”; depending on the risk, you might want to encrypt it by specifying a password
- After generation finished, the public key should be located in “`/home/<username>/.ssh/id_ed25519.pub`”
  (or at “`/home/<username>/.ssh/id_rsa.pub`”)
- Please explain that the “`.pub`” file is the public key (and can be given away / uploaded) and that the other file (with no ending) is the private key and needs to be protected.
- Copy (all!) the contents of the public key file, if you want to upload the SSH-key somewhere
  - TU GitLab: https://git.tu-berlin.de/-/user_settings/ssh_keys (click on your user icon → Preferences → SSH Keys → Add new key)
  - GitHub: https://github.com/settings/ssh/new (click on your user icon → Settings → SSH and GPG keys → New SSH key)

Useful Software

- **Git**: “`sudo apt install git`” and then
  “`git config --global user.name “<your name>”`” and
  “`git config --global user.email “<your email>”`”
- **Flatpaks** (can be easily installed on Ubuntu): https://flathub.org/setup/Ubuntu
  “`sudo apt install flatpak gnome-software-plugin-flatpak`”
  and then
  “`flatpak remote-add --if-not-exists flathub https://dl.flathub.org/repo/flathub.flatpakrepo`”