

Sicherer Fernzugriff dank Linux - selbst auf ein Windows XP



Chemnitzer LinuxTage 2025
22. März 2025

Niemand muss mitschreiben!

- Meine Slides werden im Nachgang zum Download angeboten
- Hoffentlich auf der CLT-Seite
- Mindestens aber auf der X2Go-Wiki-Events-Seite
<https://wiki.x2go.org/doku.php/events:start>
(siehe auch QR-Code)
- QR-Code kommt auch gegen Ende nochmal
- Aufpassen: Nächstes Jahr bekommt die Seite einen neuen Inhalt → am Seitenende auf 2025 klicken, um ins Archiv zu wechseln



Event-Wikiseite

(Vorerst letzter?)
Teil einer Vortragsreihe rund um
Fernzugriff, X2Go und RDP

Vortragsübersicht

Raspberry Pi Compute Module 4/Compute Module 5 ← das sind wir!
(techniklastig):

Chemnitzer LinuxTage, TU Chemnitz, 22. März 2025

Wieso/Weshalb/Warum – und die Kosten
(einsteigertauglich):

IT-Kongress, Hochschule Neu-Ulm, 07.11.2024

Raspberry Pi 4/5 im USB-Gadget-Modus
(totaler Nerdvortrag):

Interfug Chemnitz, 13.10.2024

Raspberry Pi 3/4/5 mit USB-Dongle
(techniklastig):

KieLux, 21.09.2024 & LinuxDay.AT 28.09.2024

Embedded Hardware
(techniklastig):

Tux-Tage, 02.11.2024



YouTube-Playlist
mit allen Vorträgen

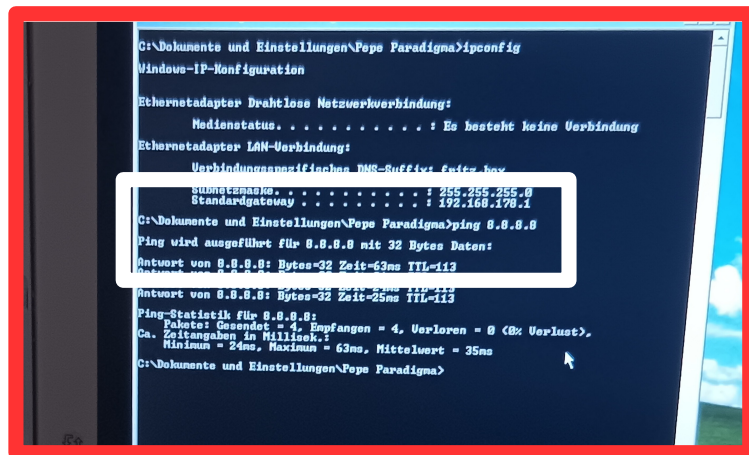
Vorstellung Stefan Baur



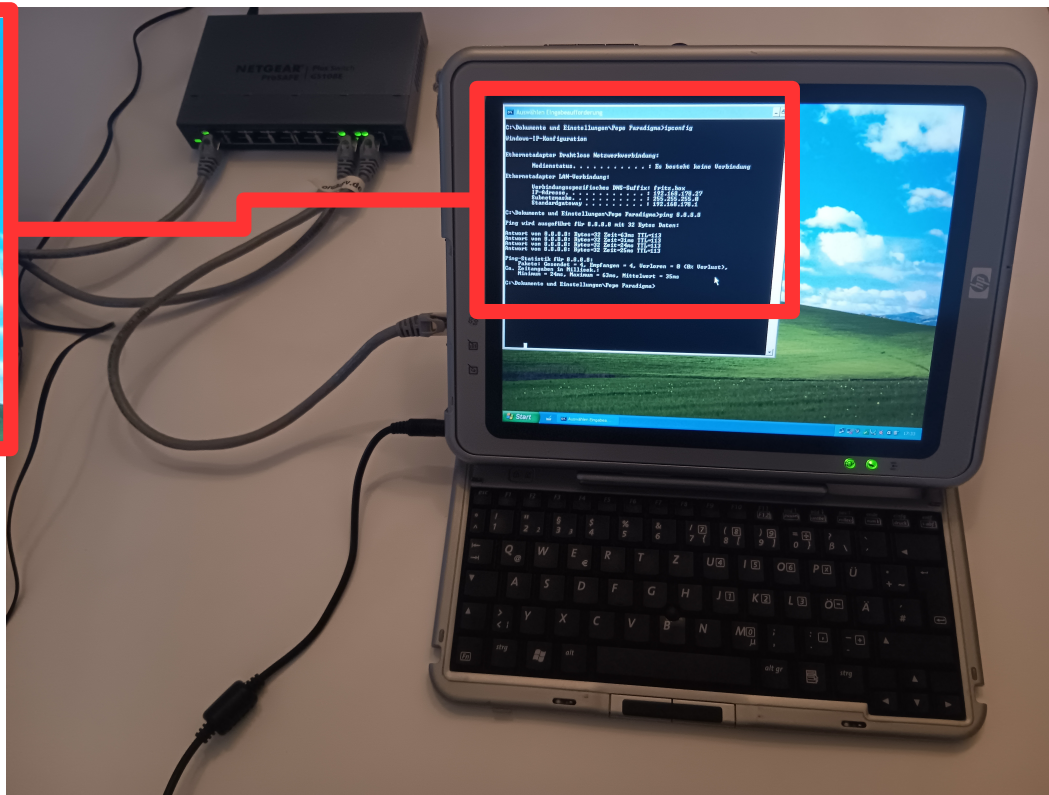
ct magazin für
computer
technik

heise online **Make:**

Das hier gilt es zu vermeiden



- Windows XP direkt im LAN, mit vollem Internetzugang
- Portforwarding aus Sicherheitsgründen natürlich nicht aktiviert
- Video „XP direkt im Internet“: <https://youtu.be/6uSVVCmOH5w>



Einfachster Softwareansatz: SSH+2FA

- Vorgeschaltetes Linuxsystem mit Secure Shell (SSH)
 - Unterstützt aktuelle, sichere Verschlüsselungstechniken
 - Unterstützt Pluggable Authentication Modules (PAM)
 - Dadurch Zwei-Faktor-Authentisierung sehr einfach möglich
 - Anbindung an LDAP oder AD zwecks Benutzerauthentisierung ebenfalls möglich (ob für diesen Zweck sinnvoll, sei dahingestellt)



Netzwerk: Welcher Paranoialevel?



Hardware: Für dieses Szenario egal

- Wenn bereits Virtualisierung im Einsatz ist, könnte man das per VM machen – aber: Sicherheitsrisiko, VM-Ausbruch-Exploits, Spectre, Meltdown, Rowhammer, etc. → besser auf „echtem Blech“
- Älterer PC, den man gegebenenfalls noch mit ein, zwei Netzwerkkarten aufrüstet → Kostenpunkt: Stromverbrauch
- Irgendwelche Custom-Embedded-Hardware (so lange von der Distribution noch unterstützt, auch 32-Bit-Hardware „recyclebar“)
- Raspberry Pi: gegebenenfalls mit separatem USB-Ethernet-Adapter für zweiten LAN-Port, oder USB-Ethernet-Gadget-Funktion des Pi 4/Pi 5, oder mit Compute Module 4/Compute Module 5 und einem Dual-Gbit/s-Baseboard.

Hardware: Lösungsansätze

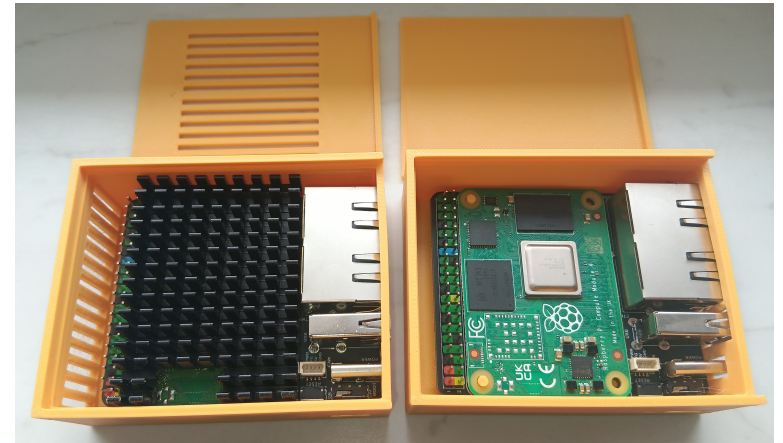


Weitere Embedded-Hardware

Raspberry Pi CM4/5
mit 2 x 1 Gigabit/s
Baseboard (Image auf
Raspberry Pi4/5 testen,
dann in MMC flashen)



3D-gedruckter Gehäuse-
entwurf (im Entstehen)
Variante mit Luftschlitzen
für CM5 mit Kühlkörper
Link zum STL bald im Wiki



Tipps & Tricks für stabilen Betrieb

- 1) CM4/CM5 mit Onboard-Flash kaufen und davon booten!
 - Nicht von microSD! → zu anfällig für 24/7-Betrieb!
 - Flash-Boot ist gar nicht soooo kompliziert!
- 2) RasPi-internen Watchdog aktivieren
 - Automatische Resets bei Hängenbleiben
- 3) Overlay-Filesystem aktivieren
 - Hartes Ausschalten könnte das Dateisystem beschädigen

Vorbereitung „CM-Betankung“

Man braucht ein USB-C-USB-A-Kabel und einen „normalen“ Pi (Pi 3 aufwärts empfohlen; 400/500 gehen auch), oder einen PC/Mac zum Betanken

- Pi geht am Einfachsten:
`sudo apt update && sudo apt install rpiboot rpi-imager`
- Windows:
 - <https://www.raspberrypi.com/software/> → rpi-imager herunterladen & installieren
 - https://files.waveshare.com/upload/f/f3/Rpiboot_setup.zip → rpiboot für Windows herunterladen & installieren
- macOS:
 - <https://www.raspberrypi.com/software/> → rpi-imager herunterladen & installieren
 - <https://www.jeffgeerling.com/blog/2020/flashing-raspberry-pi-compute-module-on-macos-usbboot> → rpiboot selbst kompilieren & installieren
- Linux:
 - Entweder rpiboot und rpi-imager per snap installieren: `snap install rpiboot && snap install rpi-imager`
 - Oder unter Ubuntu/Debian/Devuan:
 - das rpi-imager-*.deb von <https://www.raspberrypi.com/software/> herunterladen & installieren
 - rpiboot selbst kompilieren & installieren:
`sudo apt install git libusb-1.0-0-dev pkg-config build-essential && \`
`git clone --recurse-submodules --shallow-submodules --depth=1`
`https://github.com/raspberrypi/usbboot && \`
`cd usbboot && make && sudo make install`

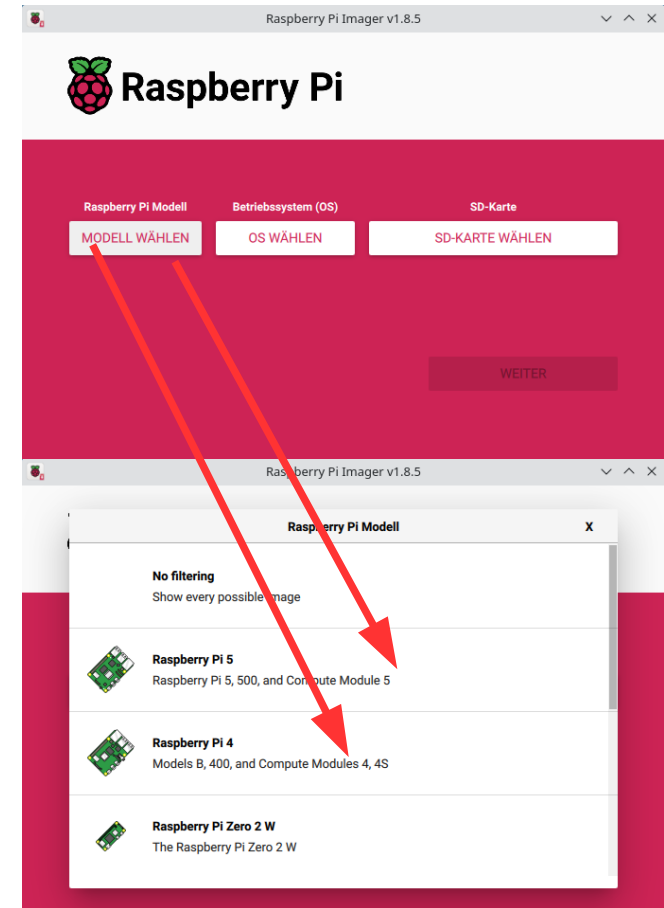
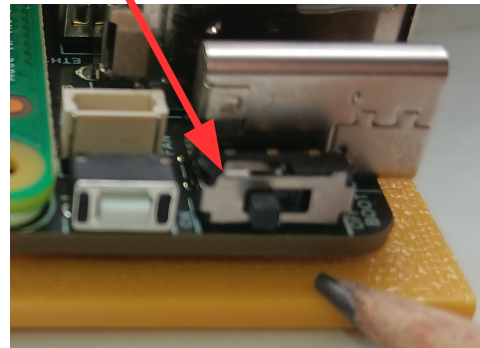
Installation auf CM mit rpi-imager (1)



Wichtig - Reihenfolge einhalten:

- 1) Schiebeschalter nach hinten (Richtung GPIOs) schieben
- 2) USB-Kabel in USB-C-Port am CM-Baseboard stecken
- 3) USB-Kabel in USB-A-Port an Pi/PC/Mac stecken
- 4) An der Shell: `sudo rpiboot`
- 5) Warten, bis Prompt wieder erscheint
- 6) An der Shell: `sudo rpi-imager`

→ Sonst findet der Imager das Compute Module nicht!



Installation auf CM mit rpi-imager (2)

The screenshots illustrate the following steps in the Raspberry Pi Imager v1.8.5 application:

- Main Screen:** Shows the Raspberry Pi logo and three tabs: **Raspberry Pi Modell** (RASPBERRY PI 5), **Betriebssystem (OS)** (OS WÄHLEN), and **SD-Karte** (SD-KARTE WÄHLEN). A red arrow points from the **OS WÄHLEN** tab to the next screen.
- Betriebssystem (OS) Selection:** A list of operating systems is shown. The first option, **Raspberry Pi OS Lite (64-bit)**, is highlighted. A red arrow points from this option to the next screen.
- SD-Karte Selection:** A list of storage devices is shown. The first option, **mmcblk0 Raspberry Pi multi-function USB device (bootfs, rootfs, homefs)**, is highlighted. A red arrow points from this option to the next screen.
- SD-Karte Selection:** The same list of storage devices is shown, but the second option, **Raspberry Pi OS LITE (64-BIT)**, is now selected. A red arrow points from this selection back to the main screen.
- Main Screen:** The **SD-KARTE WÄHLEN** tab is now selected. A red arrow points from this tab to the final step.

Installation auf CM mit rpi-imager (3)

Raspberry Pi Imager v1.8.5

Raspberry Pi

OS Anpassungen anwenden?

Möchten Sie die vorher festgelegten OS Anpassungen anwenden?

EINSTELLUNGEN BEARBEITEN NEIN, EINSTELLUNGEN LÖSCHEN

Wichtig - Reihenfolge einhalten:

- 1) Wenn Betankung beendet (Tonsignal), USB-Kabel aus USB-C-Port ausstecken
- 2) Schiebeschalter nach vorn (Richtung USB-C-Port) schieben
- 3) Ethernet-Kabel in rechten Ethernet-Port stecken
(Buchsenreihenfolge: USB-C; USB-A, eth1, eth0)
- 4) Netzteil in USB-C-Port stecken

→ Sonst bootet das Compute Module anschließend nicht!

ALLGEMEIN DIENSTE OPTIONEN

☒ Hostname: cm5-vorschaltpi .local

☒ Benutzername und Passwort festlegen

Benutzername: userle

Passwort: ●●●●●●●●

☐ Wifi einrichten

SSID: _____

Passwort: _____

☐ Passwort anzeigen ☐ Verborgene SSID

Wifi-Land: GB

☒ Spracheinstellungen festlegen

Zeitzone: Europe/Berlin

Tastaturlayout: de

SPEICHERN

DIENSTE ALLGEMEIN OPTIONEN

☒ SSH aktivieren

☐ Passwort zur Authentifizierung verwenden

☒ Authentifizierung via Public-Key
authorized_keys für 'userle': _____

SSH-KEYGEN AUSFÜHREN

Pubkey einfügen oder hier generieren lassen!

SPEICHERN

DIENSTE ALLGEMEIN OPTIONEN

☒ Tonsignal nach Beenden abspielen

☒ Medien nach Beenden auswerfen

☐ Telemetrie aktivieren

SPEICHERN

Vorarbeit auf CM-Seite

- Ihr müsst die `authorized_keys`-Datei und die `ssh-Client-Config` vom bei der Installation angelegten Standard-Benutzeraccount (`pi`, `userle`, ...) bei `root` einkopieren und das Eigentum übertragen. Nutzt dafür `ssh userle@cm5-vorschaltpi` und das Keyfile.
 - `sudo cp -a ~/.ssh /root/`
 - `sudo chown -R root:root /root/.ssh`
- Jetzt loggt ihr euch neu mit `ssh root@cm5-vorschaltpi` und dem Keyfile ein.
- Danach müsst ihr ein paar Dateien bearbeiten:
 - `/etc/network/interfaces` (und ggf. `/etc/resolv.conf`)
 - `/etc/watchdog.conf`
 - `/boot/firmware/config.txt`
 - `/boot/firmware/cmdline.txt`
 - `/etc/network/interfaces.d/eth1`
 - `/etc/dnsmasq.d/eth1` (optional)

Uplink-Interface konfigurieren

- Falls Datei komplett fehlt:
apt install ifupdown
- IP-Adresse/DNS:
 - entweder statisch auf dem System selbst eintragen mit
editor /etc/network/interfaces
und editor /etc/resolv.conf
(alles nach wie vor als root)
 - oder per DHCP zuteilen lassen
und auf dem DHCP-Server MAC
und IP fest einander zuordnen

```
root@alix1:/# cat /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
# Include files from /etc/network/interfaces.d:
source-directory /etc/network/interfaces.d
auto lo
iface lo inet loopback
```

```
allow-hotplug eth0
iface eth0 inet static
    address 192.168.178.45
    netmask 255.255.255.0
    gateway 192.168.178.1
root@alix1:/# cat /etc/resolv.conf
domain fritz.box
search fritz.box
nameserver 192.168.178.1
```

```
# Include files from /etc/network/interfaces.d:
source-directory /etc/network/interfaces.d
auto lo
iface lo inet loopback
allow-hotplug eth0
iface eth0 inet dhcp
```


Downlink-Interface konfigurieren

- Wichtig: Nicht der selbe Netzwerkbereich wie an eth0!
- Falls Verzeichnis fehlt, anlegen (Und prüfen: ifupdown installiert?):
`mkdir /etc/network/interfaces.d`
- Datei erstellen (nach wie vor als root):
`editor /etc/network/interfaces.d/eth1`
- Inhalt:
`allow-hotplug eth1`
`iface eth1 inet static`
`address 192.168.134.1`
`netmask 255.255.255.0`

Wichtig: Keine Zeile
gateway a.b.c.d
am Ende eintragen,
da Routing (und NAT)
unterbleiben soll!

Option: DHCP (dnsmasq) installieren

- Besonders bequem für die XP-Seite:
Adressvergabe per DHCP mit dnsmasq auf dem Pi
- Benötigte Befehle (alles nach wie vor als root):
`apt update && apt install dnsmasq`
`editor /etc/dnsmasq.d/eth1`

Option: DHCP (dnsmasq) einrichten

- Kein DNS, keine default Route, nur eine freie IP
- Oktett 1-3 der IP unten passend zu der IP aus `/etc/network/interfaces.d/eth1` wählen
- Datei `/etc/dnsmasq.d/eth1` mit diesem Inhalt befüllen:

```
port=0
```

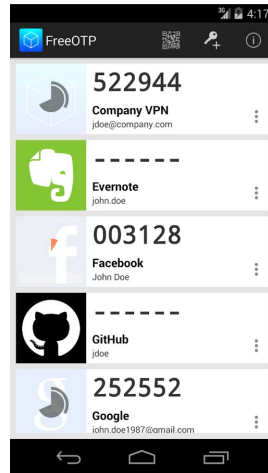
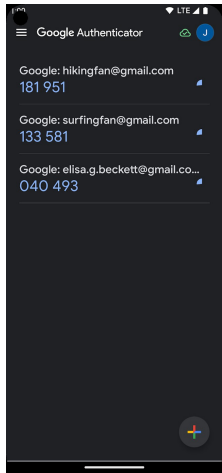
```
dhcp-option=6
```

```
dhcp-option=3
```

```
dhcp-range=192.168.134.2, 192.168.134.2, 12h
```

Mögliche zusätzliche Faktoren

- 2FA über mehrere PAMs möglich (u.a. Handy-Apps, Hardware-Token)



- Google-Modul libpam-google-authenticator ist ziemlich komfortabel (bietet Recovery-Codes, telefoniert nicht nach Hause, Open Source)

2FA detailliert erklärt

→ KieLux-2024-Video und „Spickzettel“
am Ende dieser Slides



Direkt zur entsprechenden
Stelle im KieLux-2024-Video
(Sprungmarke in der URL)



KieLux-Eintrag auf der
2024er Event-Seite im X2Go-Wiki
(mit Links zu Folien und Video)

Dort „Einrichtung SSH+2FA (Teil 1)“ bis „Einrichtung SSH+2FA (Teil 7)“
(Folie 9 ff.)

Der erste Login mit 2FA

- Siehe da, es klappt (Screenshot von anderer Hardwareplattform):

```
1 user@hpwendy:~$ ssh userle@alix1
2 Password:
3 Verification code:
Linux alix1 6.1.0-21-686 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) i586

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jun 20 13:05:51 2024 from 192.168.0.14
userle@alix1:~$
```

Watchdog installieren & konfigurieren

- Watchdog-Tool installieren (als root)
`apt install watchdog`
- Watchdog konfigurieren (als root)
`editor /etc/watchdog.conf`
- **Wert ändern**/Kommentarzeichen (#) entfernen:
`watchdog-device = /dev/watchdog`
`watchdog-timeout = 15`
`max-load-1 = 24`
- Watchdog aktivieren (als root)
`editor /boot/firmware/config.txt`
- Diesen Block am Ende einfügen:
`[all]`
`# enable Hardware Watchdog`
`dtparam=watchdog=on`
- Ab dem nächsten Neustart ist der Watchdog aktiv

Overlay-Dateisystem

- Vorteile:
 - Schadcode überlebt (hoffentlich) den nächsten Neustart nicht
 - Dateisystem ist beim Start immer in einem sauberen Zustand
- Nachteile:
 - Vor Updates muss auf read-write geschaltet werden, danach zurück
 - Benutzerverzeichnis braucht andere Konfiguration, da Schreibzugriff/
Persistenz notwendig (/home als Mountpoint, mit rw, sync, noexec),
u.a. für die Google-Authenticator-Daten
→ Sonst sind nach Neustart die verbrauchten Codes wieder aktiv!

Persistente Homedirectories

- CM herunterfahren, Flash-Schalter umlegen, per USB-Kabel an anderen Rechner anschließen, rpiboot starten
- CM z.B. mittels `gparted /dev/disk/by-id/*Raspberry*:0` umpartitionieren:
Partition 2 (ext4, Label „rootfs“) schrumpfen und in freiem Platz Partition 3 (ext4, Label "homefs") anlegen und formatieren
- USB-Kabel abziehen, Schalter wieder umlegen, CM booten, als root einloggen
(nicht su oder sudo als Benutzer – sonst ist /home in Nutzung und damit blockiert)
- Auf dem CM diese Befehle eingeben (das zieht die Homedirectories um):

```
mount /dev/mmcblk0p3 /mnt && mv /home/* /mnt && umount /mnt && \  
echo -e "/dev/mmcblk0p3\t/home\ttext4\ttrw, sync, noexec, defaults\t0\t2" \  
>> /etc/fstab && mount -a
```

Habt ihr es richtig gemacht,
gibt es genau einen Match!

Schreibschutz aktivieren

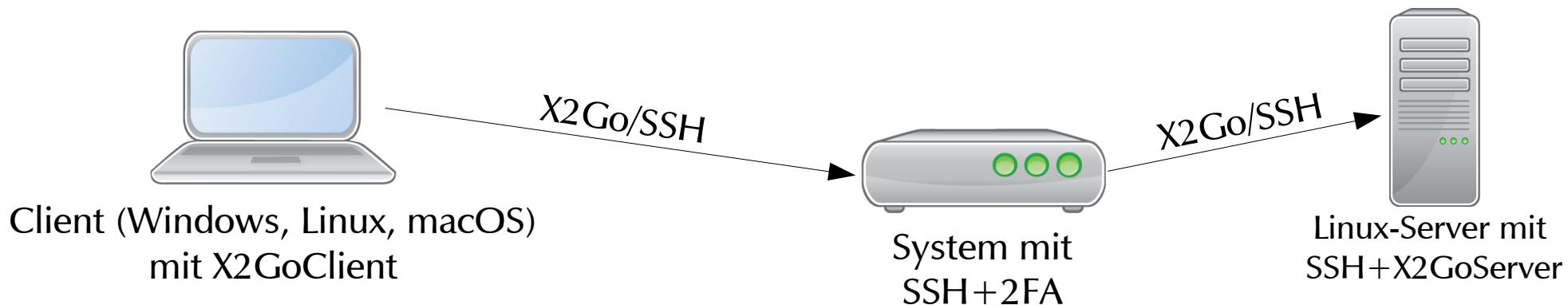
- Als root den Befehl `raspi-config` aufrufen
 - Performance Options
 - Overlay File System: enable → Yes
 - Boot Partition: write-protected → No
 - Finish

→ Reboot now: No

Wichtig!

- Patchen um Homedirectories auszuklammern, dann Neustart auslösen:
`sed -e "s/^overlayroot=tmpfs/overlayroot=tmpfs:recurse=0/" \`
`-i /boot/firmware/cmdline.txt && reboot`
- Achtung: `raspi-config` kann das aktuell nicht deaktivieren → wie's trotzdem geht, kommt weiter unten auf Slide „Installation X2GoServer & rdesktop“

System nur als SSH-Proxy/Jumphost



- Details dazu im KieLux-Vortrag:
„X2Go – und die Welt wird bunt“, Folie 37, bis
„Und nun ...“, Folie 42
- Hilft uns für Windows so noch nicht weiter
- Trotzdem ein kurzer Blick darauf, wie das aussieht



Direkt zur entsprechenden
Stelle im KieLux-Video
(Sprungmarke in der URL)

Was ist X2Go

- X2Go ist eine freie Remote-Desktop-/Remote-Application-Lösung
→ kostenlos nutzbar, auch in Firmen, eigene Anpassungen erlaubt
- X2GoClient gibt es für Linux, Windows und macOS
 - Er kann auch als grafisches Frontend für RDP- (Windows Remote Desktop)/XDMCP-Logins dienen → das schauen wir uns nachher an!
 - Der Linux-X2GoClient eignet sich auch zum Direktzugriff auf RDP und XDMCP – ohne X2GoServer
- X2GoServer gibt es aktuell nur für Linux → ist für den heutigen Vortrag aber nicht wirklich relevant

Konfiguration X2GoClient - SSH-Proxy

- Host: Die *interne* IP-Adresse des X2Go-Servers
- Häkchen „Proxy-Server für SSH-Verbindung verwenden“ ankreuzen
→ Weitere Optionen klappen aus
- Typ: SSH
- Host: Die *öffentliche* IP-Adresse des Routers (auf diesem muss ein Portforwarding eingerichtet werden)
- Login: pi bzw. userle

The screenshot shows the X2GoClient configuration window with the following settings:

- Sitzung:** Sitzungsnamen: X2GoServer-Firma
- Verbindung:** Pfad: /
- Server:**
 - Host: 192.168.178.123
 - Login: meinx2goserverbenutzername
 - SSH-Port: 22
 - RSA/DSA-Schlüssel verwenden (ssh):
 - ☐ Anmeldung über voreingestellten SSH-Schlüssel oder ssh-agent
 - ☐ Kerberos5 (GSSAPI) Authentifizierung
 - ☐ Übertragung der GSSAPI-Legitimation auf den Server
 - ☒ Proxy-Server für SSH-Verbindung verwenden
- Proxy-Server:**
 - Typ: ☒ SSH
 - ☐ HTTP
 - Gleiche Anmeldung wie für X2Go-Server: ☐
 - Gleiches Kennwort wie für X2Go-Server: ☐
 - Login: userle
 - Host: öffentliche.ip.hier
 - Port: 22
 - RSA/DSA-Schlüssel:
 - ☐ SSH-Agent oder SSH-Standardschlüssel
 - ☐ Kerberos5 (GSSAPI) Authentifizierung
- Sitzungsart:**
 - ☐ In X2GoKDrive starten (experimentell)
 - XFCE
 - Befehl:

Buttons at the bottom: OK, Abbrechen, Voreinstellungen

SSH-Prozess <@kdrive-server>

Anwendungen: doc.newtox2go [X2G... xclock xeyes

2024-06-20 19:11 Ben Utzer

doc.newtox2go [X2Go - everywhere@home] - Pale Moon

File Edit View History Bookmarks Tools Help

x2go.org <https://wiki.x2go.org/doku.php/doc.newtox2go> DuckDuckGo

Most Visited: Pale Moon, Pale Moon forum, F.A.Q., Release notes

doc.newtox2go [X2Go - every

Announcements / News

Documentation

- New to X2Go? Start here!
- Success Stories
- Installing X2Go
- Using X2Go
- Desktop Environment
- Compatibility
- Windows-Specific Release Notes
- Participate in X2Go
- Who is who in X2Go
- Professional Support
- Development Sponsoring
- Frequently Asked Questions
- HowTos

Download

New to X2Go? Start here!

Overview

X2Go enables you to access a *graphical desktop* of a computer over a *low bandwidth* (or high bandwidth) connection.

X2Go is a *Remote Desktop* solution, which some vendors vaguely call *Remote Control*. This is not to be confused with Microsoft Remote Desktop Connection, which is a competing Remote Desktop solution and protocol.

More of Contents

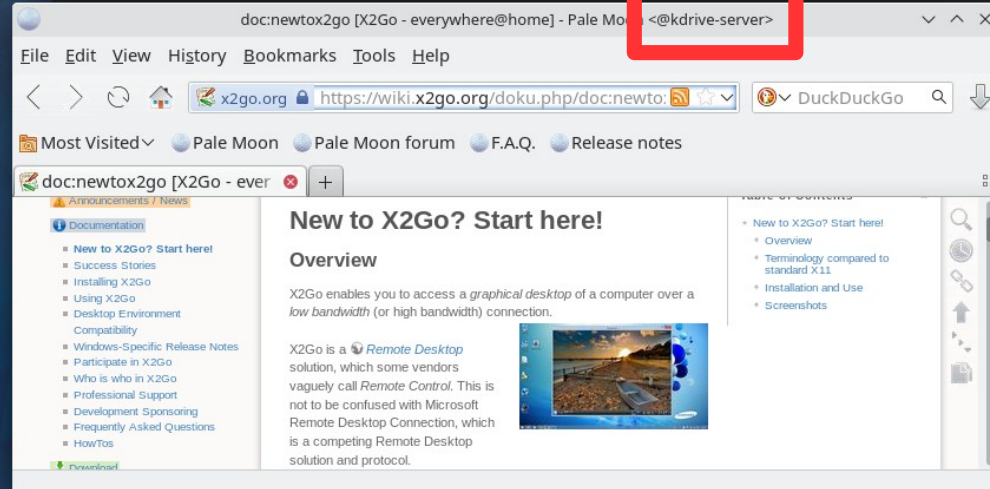
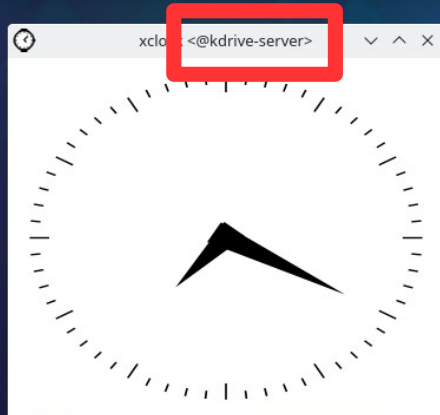
- New to X2Go? Start here!
- Overview
- Terminology compared to standard X11
- Installation and Use
- Screenshots

X2Go per Spende unterstützen?
Spendenlinks auf <https://wiki.x2go.org>
oder via QR-Code hier:




```
~: bash — Konsole
Datei Bearbeiten Ansicht Lesezeichen Module Einstellungen Hilfe
Neues Unterfenster Split View Kopieren Einfügen
tuebix2024@hpwendy:~$ x2golistsessions
tuebix2024@hpwendy:~$
```

```
~: xclock — Konsole <@kdrive-server>
Datei Bearbeiten Ansicht Lesezeichen Module Einstellungen
Neues Unterfenster Ansicht teilen Kopieren Einfügen Suchen
user1@kdrive-server:~$ x2golistsessions
320679|user1-50-1718903626_strPUBLISHED_dp24|50|kdrive-server|R|2024-06-20T19:13:46|e9cd222b4286d6b3020bcf6275
2d9e90|192.168.133.100|54841|54842|2024-06-20T19:13:47|user1|354|54843|-1|-1
user1@kdrive-server:~$ xclock
```



Und nun, das Wett... äh, Windows

- X2Go unterstützt die alten, unsicheren Windows-Versionen (ohne Network Level Authentication) direkt.
- Um keinen weiteren Server zu benötigen, installieren wir x2goserver und rdesktop auf unserem Vorschaltssystem und machen es zu einem X2Go-Server.
- Hinweis zur Schreibweise:
 - X2GoServer = die Software
 - X2Go-Server = das Linux-System, auf dem die X2GoServer-Software installiert ist

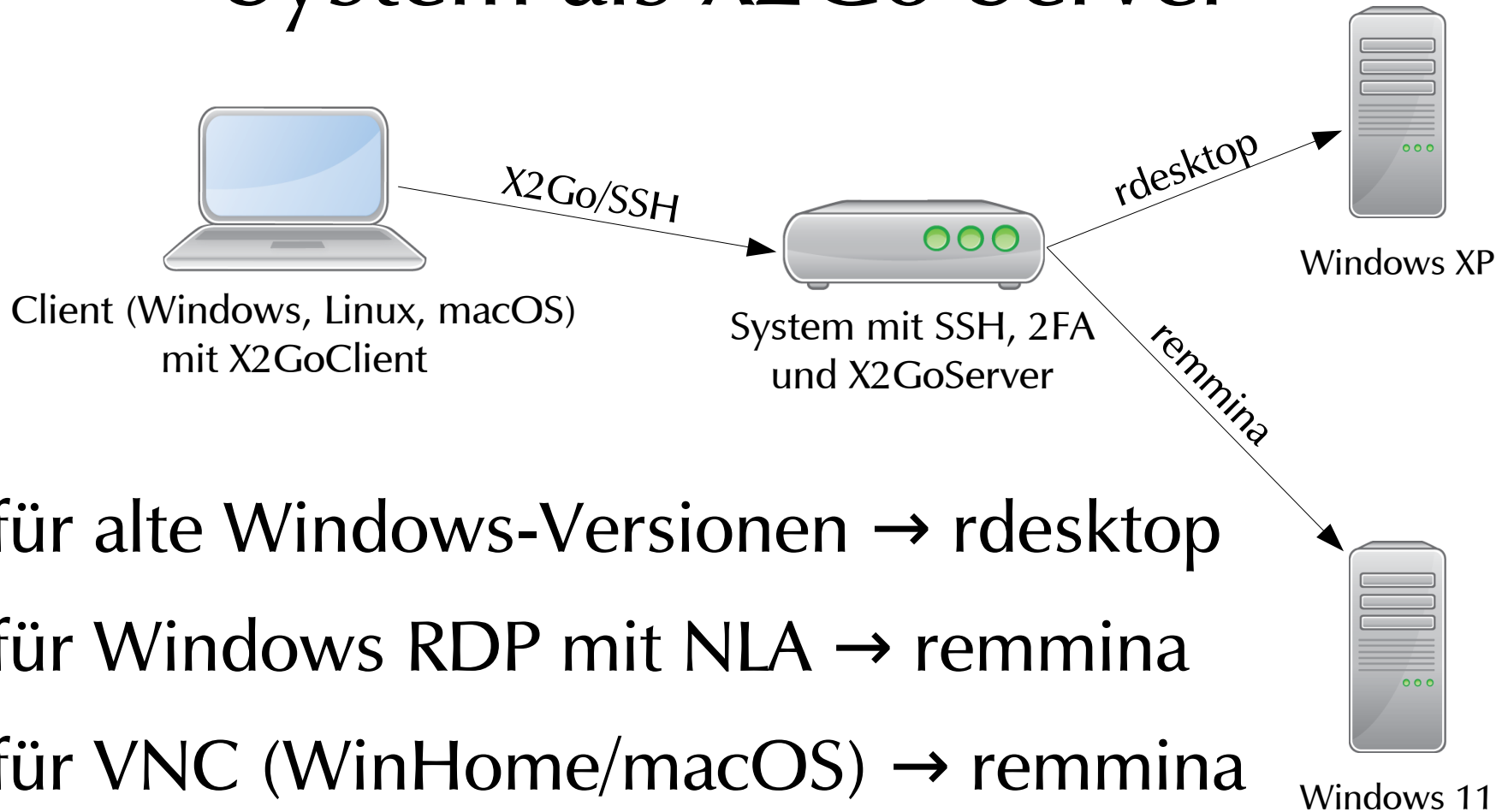
Installation X2GoServer & rdesktop

- Als root das overlayroot wieder abschalten und Neustart auslösen:

```
sed -e "s/^overlayroot=tmpfs[^\ ]* //" \  
-i /boot/firmware/cmdline.txt && reboot
```
- Optional das X2Go-Stable- bzw. Nightly-Repository einbinden
(Anleitung: <https://wiki.x2go.org/doku.php/wiki:repositories:raspbian>)
- Achtung: Derzeit gibt es Raspi-X2Go-Pakete nur von Raspberry Pi OS selbst oder im X2Go-Nightly-Repo, aber noch nicht in X2Go-Stable!
- Nicht vergessen: Distributionsname auf bookworm ändern
- Dann als root bzw. jeweils mit vorangestelltem sudo vor apt:

```
apt update && apt install x2goserver x2goserver-xsession rdesktop
```
- Danach wieder das overlayroot einschalten/patchen und neu starten

System als X2Go-Server



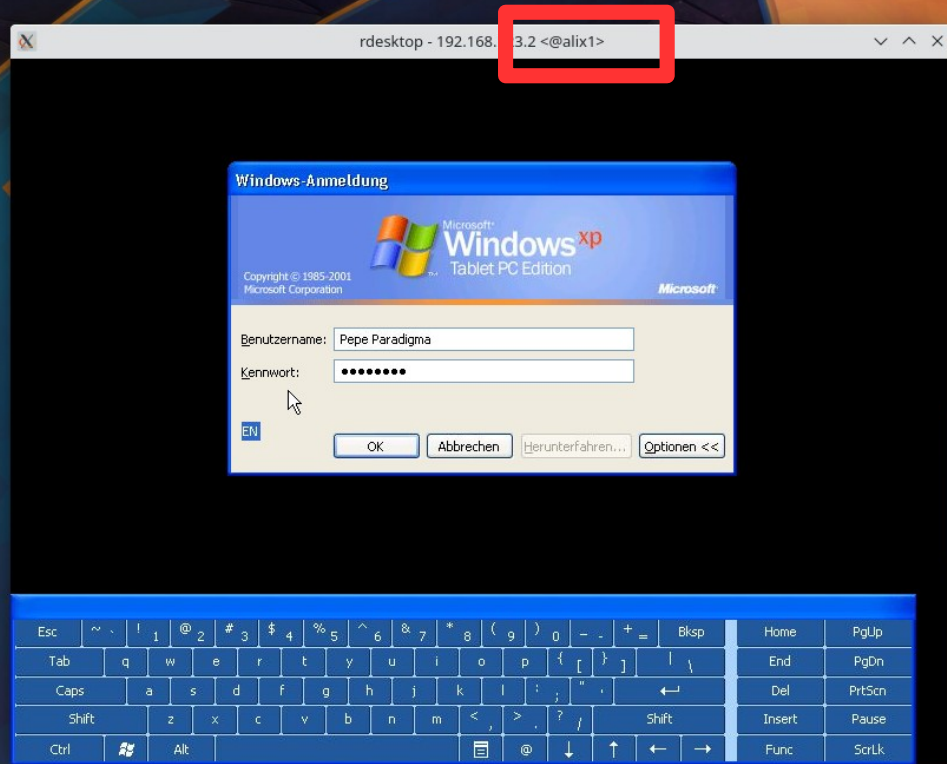
Konfiguration X2GoClient - rdesktop

- Host: Die *öffentliche* IP-Adresse des Routers (auf diesem muss ein Portforwarding eingerichtet werden)
- Login: pi bzw. userle
- Häkchen „Proxy-Server für SSH-Verbindung verwenden“ *nicht* ankreuzen
- Sitzungstyp:
Verbindung mit Windows-Terminalserver herstellen/IP des Windows-PCs

The screenshot shows the X2GoClient configuration window with the following settings highlighted by red boxes:

- Host:** 192.168.178.23
- Login:** userle
- SSH-Port:** 22
- Proxy-Server für SSH-Verbindung verwenden:** ☐ (unchecked)
- Sitzungsart:** ☐ In X2GoDrive starten (experimentell) (unchecked); **Verbindung mit Windows Terminalserver herstellen** (selected); **Server:** 192.168.178.23

Other visible settings include: Sitzung: Verbindung; Sitzungsname: JumpHost-Firma; Pfad: /; RSA-/DSA-Schlüssel verwenden (ssh): [empty]; and buttons for OK, Abbrechen, and Voreinstellungen.



X2GoClient

Sitzung Einstellungen Hilfe

Sitzungs-ID: userle-50-1718906182_stRRDP_dp24
Server: 192.168.133.1
Login: userle
Display: 50
Startzeit: Do, Juni 20 19:57:28 2024
Status: aktiv

Info: Using ZLIB stream compression 4/4.
Info: No suitable cache file found.
Info: Forwarding X11 connections to display ':0'.
Info: Forwarding auxiliary X11 connections to display ':0'.
Session: Session started at 'Thu Jun 20 19:57:28 2024'.
Info: Established X server connection.
Info: Using shared memory parameters 0/0K.

☒ Zeige Details



rdesktop - 192.168.133.2 <@alix1>

Papierkorb
Bluetooth-Umgebung
Mozilla Firefox

Eingabeaufforderung

```
C:\Dokumente und Einstellungen\Pepe Paradigma>ipconfig

Windows-IP-Konfiguration

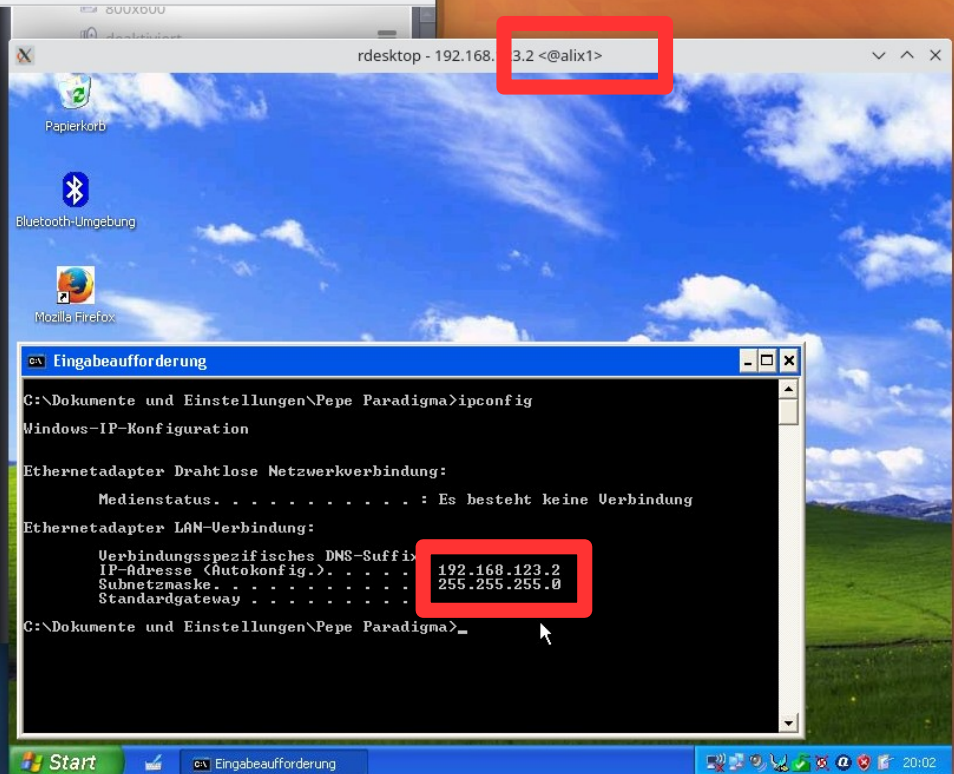
Ethernetadapter Drahtlose Netzwerkverbindung:

    Medienstatus. . . . . : Es besteht keine Verbindung

Ethernetadapter LAN-Verbindung:

    Verbindungsspezifisches DNS-Suffix: 
    IP-Adresse (Autokonfig.) . . . . . : 192.168.123.2
    Subnetzmaske . . . . . : 255.255.255.0
    Standardgateway . . . . . : 

C:\Dokumente und Einstellungen\Pepe Paradigma>
```



Vorteil remmina

- Eine Anmeldung, mehrere Verbindungen – auch gleichzeitig
- Kann nicht nur RDP (auch mit NLA!), sondern auch VNC sprechen
- VNC lässt sich auch auf Windows Home oder macOS nutzen, aber:
 - VNC ist
 - Meistens nicht verschlüsselt → SSH ändert das auf der WAN-Strecke
 - Deutlich träger als X2Go → X2Go ändert das auf der WAN-Strecke
- Dank X2Go muss Remmina nicht auf dem Client zur Verfügung stehen
- Die Verbindungskonfiguration ist zentral auf dem Pi hinterlegt
→ Einfache Aktualisierung durch den Admin, muss nicht aufs Endgerät

Installation remmina (RDP-NLA, VNC)

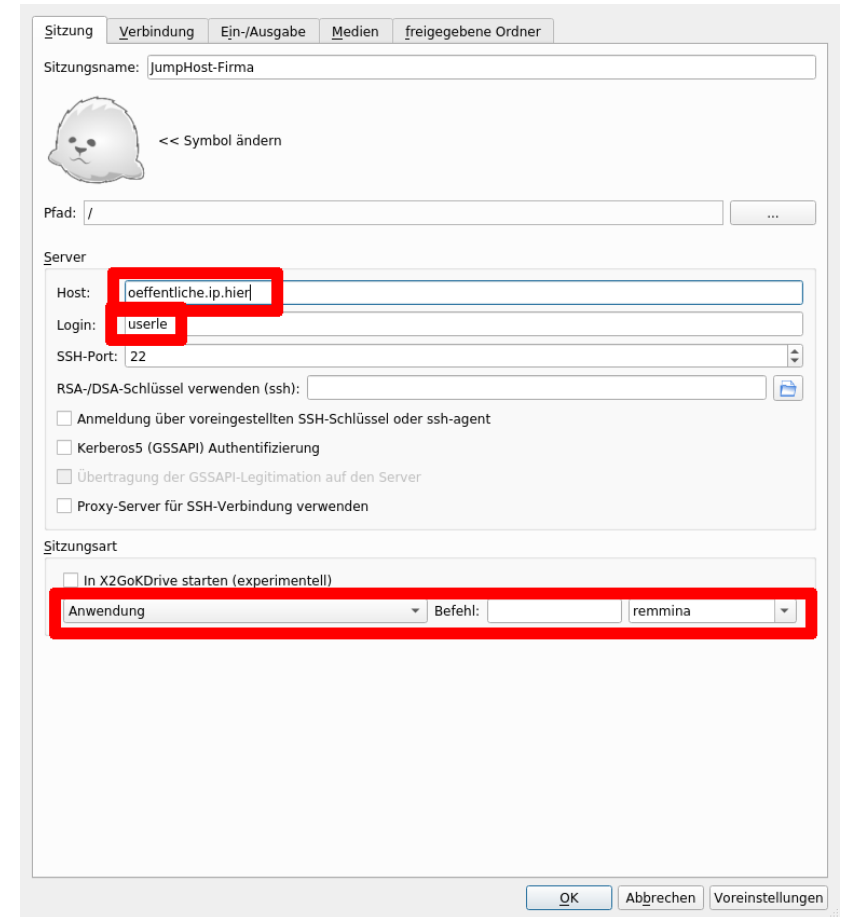
- Als root das overlayroot wieder abschalten und Neustart auslösen:

```
sed -e "s/^overlayroot=tmpfs[^\ ]* //" \  
-i /boot/firmware/cmdline.txt && reboot
```
- Dann als root bzw. jeweils mit vorangestelltem sudo vor apt:

```
apt update && apt install freerdp2-x11 remmina
```
- Danach wieder das overlayroot einschalten und neu starten

Konfiguration X2GoClient - remmina

- Host: Die öffentliche IP-Adresse des Routers (auf diesem muss ein Portforwarding eingerichtet werden)
- Login: pi bzw. userle
- Sitzungstyp: Anwendung
- Befehl:
 - erstes Feld leer lassen
 - Im Dropdown-Menü *tippen*: remmina



The screenshot shows the X2GoClient configuration window with the 'Verbindung' tab selected. The 'Sitzungsname' field contains 'JumpHost-Firma'. Below it is a small icon of a dog and a '<< Symbol ändern' button. The 'Pfad' field contains '/'. The 'Server' section has the following fields: 'Host' (containing 'oeffentliche.ip.hier'), 'Login' (containing 'userle'), and 'SSH-Port' (set to '22'). There are four checkboxes for authentication: 'RSA-/DSA-Schlüssel verwenden (ssh):', 'Anmeldung über voreingestellten SSH-Schlüssel oder ssh-agent', 'Kerberos5 (GSSAPI) Authentifizierung', and 'Übertragung der GSSAPI-Legitimation auf den Server'. The 'Sitzungsart' section has a checkbox 'In X2GoKDrive starten (experimentell)' and a dropdown menu 'Anwendung' set to 'remmina'. The 'Befehl' field is empty. At the bottom are buttons for 'OK', 'Abbrechen', and 'Voreinstellungen'.

X2GoClient

Sitzung Einstellungen Hilfe

Sitzungs-ID: userle-50-1718969159_stRemmina_dp24

Server: OSUOSL Deb11 Stable

Login: <@jarvis-pi3>

Display:

Startzeit:

Status:

Info: Using ZL

Info: Using ZL

Info: No suita

Info: Forward

Info: Forward

display ':0'.

Session: Sessi

2024'.

Info: Establish

Info: Using sh

✓ Zeige Detai

Remmina Remote Desktop Client

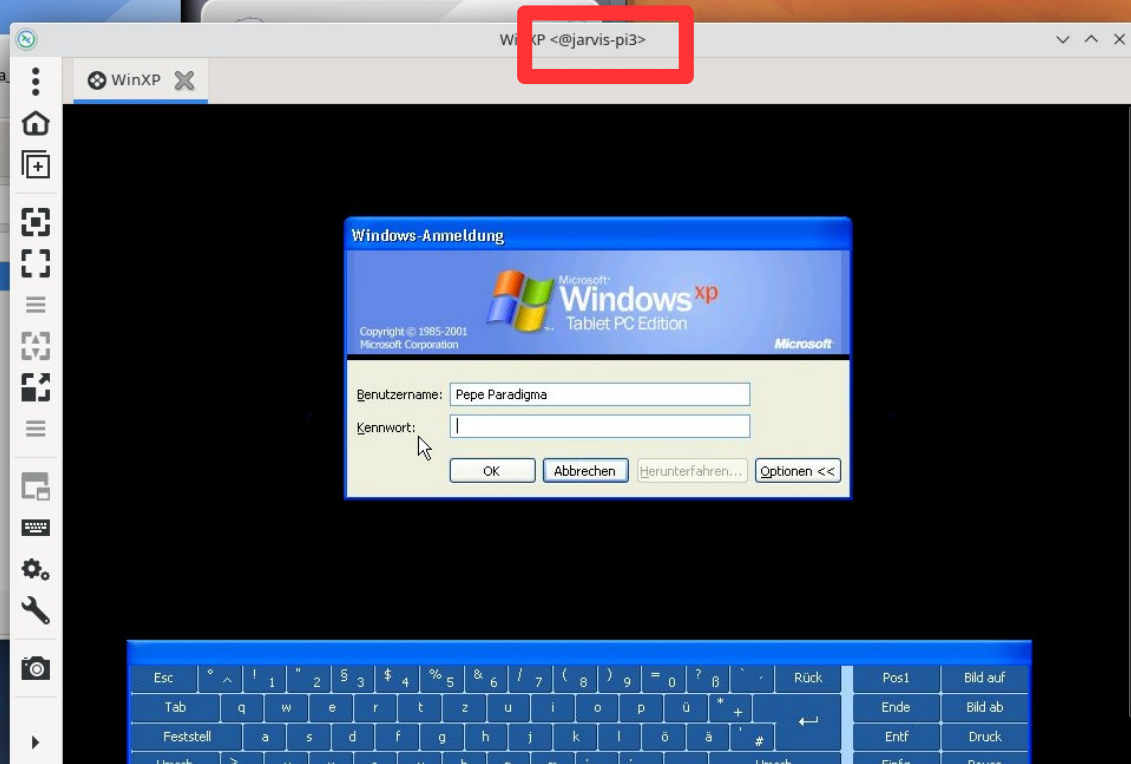
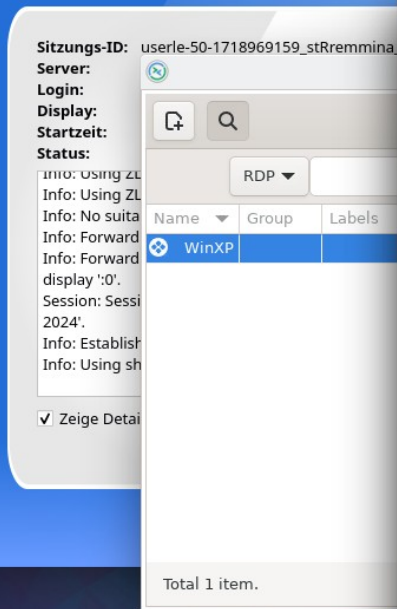
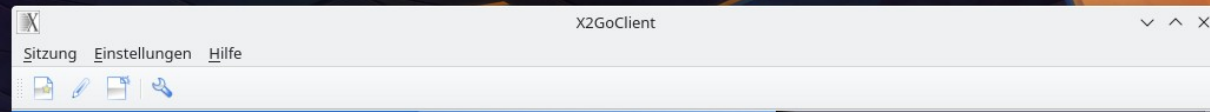
Remmina Remote Desktop Client

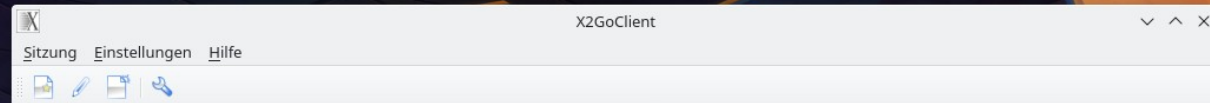
RDP

Name	Group	Labels	Server	Plugin	Last used
WinXP			192.168.123.2	RDP	2009-10-16 - 09:04:46

Total 1 item.







Sitzungs-ID: userle-50-1718969159_stRemmina_dp
Server:
Login:
Display:
Startzeit:
Status:
Info: Using ZL
Info: Using ZL
Info: No suit
Info: Forward
Info: Forward
display ':0'.
Session: Sessi
2024'.
Info: Establish
Info: Using sh

☒ Zeige Detai

RDP ▾

Name ▾	Group	Labels
WinXP		

Total 1 item.

WinXP <@jarvis-pi3>

Papierkorb

Bluetooth-Umgebung

Mozilla Firefox

Eingabeaufforderung

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Dokumente und Einstellungen\Pepe Paradigma>ipconfig

Windows-IP-Konfiguration

Ethernetadapter Drahtlose Netzwerkverbindung:

    Medienstatus. . . . . : Es besteht keine Verbindung

Ethernetadapter LAN-Verbindung:

    Verbindungsspezifisches DNS-Suffi
    IP-Adresse (Autokonfig.). . . . . 192.168.123.2
    Subnetzmaske. . . . . 255.255.255.0
    Standardgateway. . . . .

C:\Dokumente und Einstellungen\Pepe Paradigma>
```

Start | Eingabeaufforderung 13:34



Win10Home <@jarvis-pi3>

Papierkorb
UltraVNC Launcher

UltraVNC Server
PuTTY (64-bit)

Info über Windows



Microsoft Windows
Version 22H2 (Build 19045.2673)
© Microsoft Corporation. Alle Rechte vorbehalten.

Das Betriebssystem Windows 10 Home und die zugehörige
Benutzeroberfläche sind durch Marken- und andere rechtsabhängige bzw.
bestehende gewerbliche Schutz- und Urheberrechte in den Vereinigten
Staaten und anderen Ländern geschützt.

Dieses Produkt ist unter den [Microsoft-
Softwarelizenzbedingungen](#) lizenziert für:

Benutzername
Unternehmensname

OK

erle>ipconfig

Konfiguration

Adapter Ethernet:

Status : Medium getrennt
Linkspezifisches DNS-Suffix: stefanbaur.home

Adapter LAN-Verbindung* 1:

Status : Medium getrennt
Linkspezifisches DNS-Suffix:

Adapter LAN-Verbindung* 2:

Status : Medium getrennt
Linkspezifisches DNS-Suffix:

Adapter WLAN:

Linkspezifisches DNS-Suffix
Linklokale IPv6-Adresse . . . fe80::26dc:c2bc:eb48:43b%4
Adresse 192.168.0.3
Maske 255.255.255.0
Standardgateway 192.168.0.1

C:\Users\userle>

Suchen

CLXP index -0.91%

14:35
21.06.2024

DE 14:35
21.06.24

Zusammenfassung 1/2

- Wir brauchen für eine Zwei-Faktor-gesicherte Remote-Desktop-Lösung nur grob eine Handvoll über die Grundinstallation hinausgehende Pakete:

- libpam-google-authenticator und ntp

- watchdog Diese vier brauchen wir auch für die Textkonsole

- overlayroot

- dnsmasq Dieses brauchen wir nur für DHCP Richtung XP

- x2goserver und x2goserver-xsession Diese für alle Desktops

- rdesktop, freeRDP, und/oder remmina Diese nur für Windows

Zusammenfassung 2/2

- Otto Normaluser bekommt mit X2GoClient eine One-Click-Lösung (auch für Windows)
- Es funktioniert mit alten und neuen Windows-Pro- und Windows-Server-Versionen
(Und per remmina sogar mit VNC-Servern, also Windows Home und macOS)
- Es ist wartungsarm und platzsparend: Unter 4 GB belegt, selbst mit freeRDP und remmina!
- Es ist Open Source und kostenlos
- Die einzigen Kostenpunkte:
 - Hardware-Anschaffung
 - Arbeitszeit für die Installation

```
root@cm5-vorschaltpi:~# df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            2.0G   0    2.0G   0% /dev
tmpfs           405M  5.3M  400M   2% /run
/dev/mmcblk0p2  13G   3.0G   9.2G  25% /
tmpfs           2.0G   0    2.0G   0% /dev/shm
tmpfs           5.0M   48K   5.0M   1% /run/lock
/dev/mmcblk0p3  975M   68K   908M   1% /home
/dev/mmcblk0p1  510M   56M   455M  11% /boot/firmware
tmpfs           405M   0    405M   0% /run/user/0
```


Nächste X2Go-Events

- Vermutlich:
 - 26.04.2025 Linux-Info-Tag Augsburg
 - 18.-20.09.2025, KieLux, Kiel
 - 27.9.2025 LinuxDay.AT, Dornbirn
 - 13.11.2025 IT-Kongress, Hochschule Neu-Ulm
- Bestätigt:
 - 05.07.2025, TUBIX, Tübingen
- Wiki: <https://wiki.x2go.org/doku.php/events:start>



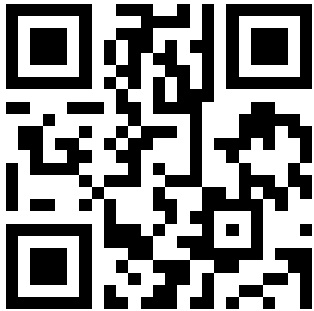
Event-
Wikiseite

X2Go lebt vom Mitmachen

- Helfer gesucht!
- X2Go kann immer zwei Dinge von euch brauchen:
 - Zeit/KnowHow – auch von Nicht-Programmierern!
 - Geld/Hardware/Dienstleistung: Man kann ...
 - über den orca e.V. (gemeinnützig) eine zweckgebundene Spende an X2Go leisten
 - eine der Firmen im Projekt mit einer konkreten Aufgabe (Bugfix, Feature Request) beauftragen

Spenden/Aufträge

- Für Spenden haben wir mehrere WirWunder/Betterplace-Seiten (Events, Infrastrukturkosten, ...) direkt auf der Wiki-Startseite: <https://wiki.x2go.org>
- Firmen, die für Aufträge zur Verfügung stehen: <https://wiki.x2go.org/doku.php/0spnn5> (null-spnn-fünf)



Spendenlink



Liste der Supportfirmen

Vielen Dank für das Interesse!
Es folgt die Q&A-Runde, eventuell mit
Live-Demo, wenn noch Zeit ist!



Spendenlink



Liste der Supportfirmen

The background is a solid blue color. At the top, there are three stylized, light blue clouds. At the bottom, there is a decorative border consisting of a series of small, light blue, scalloped shapes.

SSH+2FA-Einrichtungs-Spickzettel

Einrichtung SSH+2FA (Teil 1)

- Annahmen:
 - Basissystem ist Raspberry Pi OS 12 mit aktiviertem SSH
 - Benutzer root ist per SSH-Keyfile eingeloggt

Achtung: Als Benutzer einloggen und su oder sudo verwenden, funktioniert dafür nicht! → Wichtig, sonst sperrt man sich gegebenenfalls aus!
- Als root:
`apt update && apt install ntp libpam-google-authenticator`
(Wir brauchen ntp für die genaue Zeit, die Token sind time-based)
- Als root an das Ende der Datei `/etc/pam.d/sshd` diese Zeile anhängen:
`auth required pam_google_authenticator.so`

Einrichtung SSH+2FA (Teil 2)

- Falls außer dem beim Einrichten angelegten normalen Benutzeraccount (pi, userle, ...) noch weitere Accounts gewünscht sind, als root den/die Benutzer anlegen:
adduser nochaineruserle # oder wie der User auch immer heißen soll
- Als root die Datei /etc/ssh/sshd_config öffnen und diese Parameter setzen/prüfen (es darf kein „#“ davorstehen):
PermitRootLogin prohibit-password # kein yes
KbdInteractiveAuthentication yes
UsePAM yes
- Als root den sshd neu starten (dabei fliegt man *nicht* raus, keine Sorge):
service ssh restart

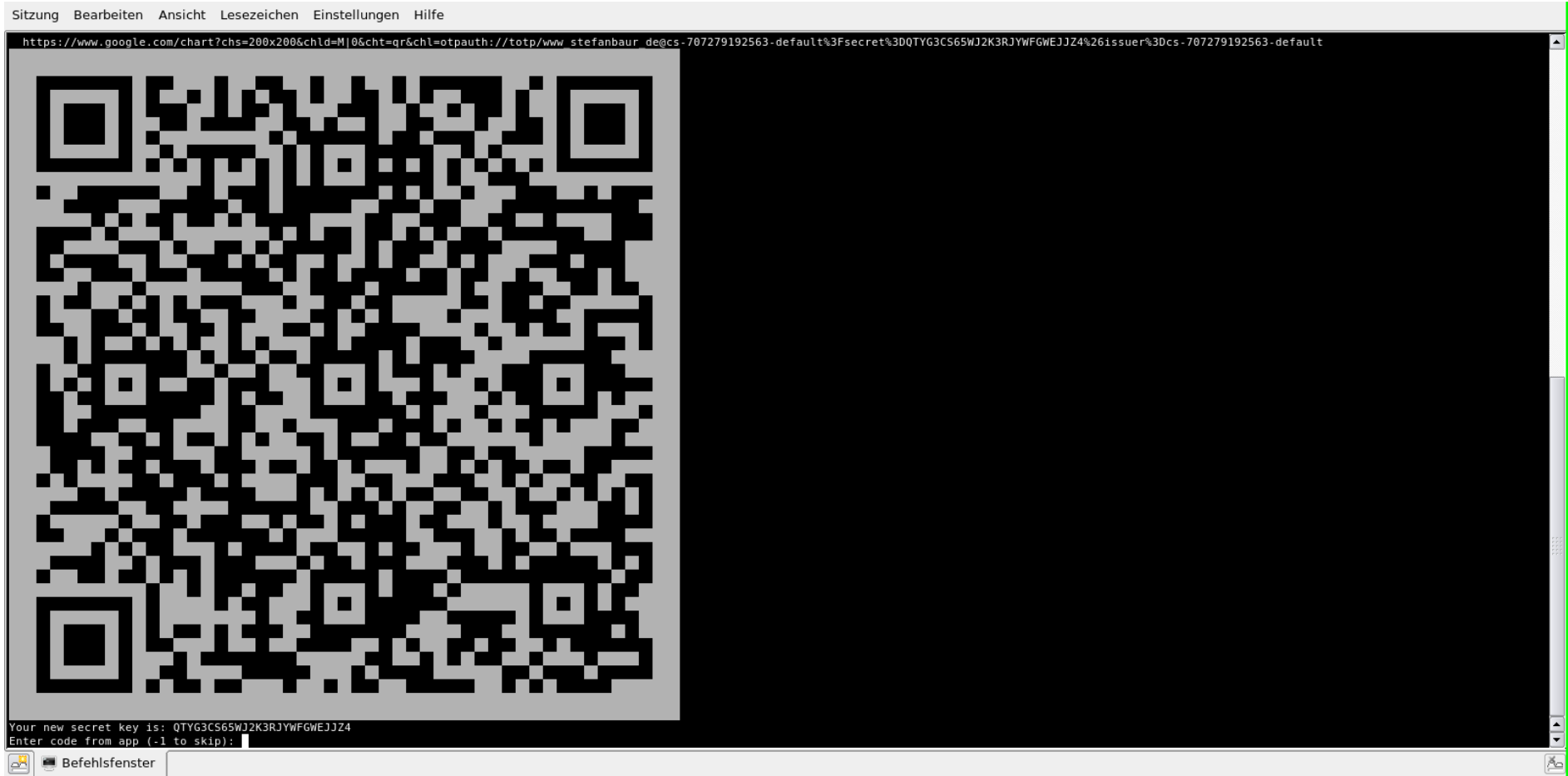
Einrichtung SSH+2FA (Teil 3)

- Als root mittels `su pi` bzw. `su userle` in den Benutzerkontext wechseln
- Als Benutzer `pi`, `userle` usw. dann jeweils die Google-Authenticator-Konfiguration starten: `google-authenticator`

Einrichtung SSH+2FA (Teil 4)

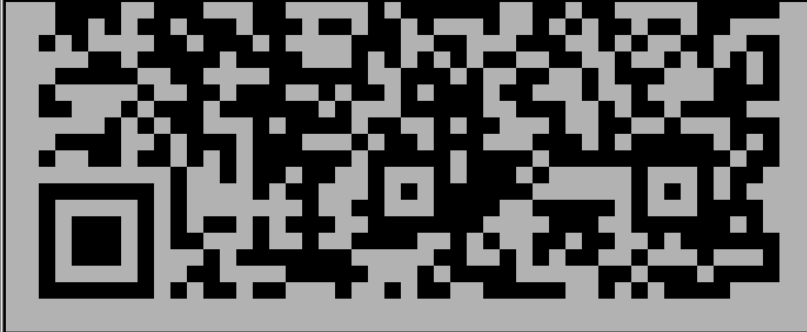
- Die Fragen des Google-Authenticator-Konfiguration pro Benutzeraccount jeweils wie folgt beantworten:
 - `Do you want authentication tokens to be time-based (y/n)` `y`
 - Danach erscheint ein QR-Code auf der Konsole
 - Diesen mit einer OTP-App wie FreeOTP+ oder Google Authenticator einlesen
- `Enter code from app (-1 to skip):`
 - Entweder einen Code aus der App zum Test eingeben
 - oder mittels `-1` den Test überspringen

Google Authenticator: QR-Code



Google Authenticator: Recovery-Code

Sitzung Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe



Your new secret key is: QTYG3CS65WJ2K3RJYWFGWEJJZ4
Enter code from app (-1 to skip): -1

Your emergency scratch codes are:

78318241
28320493
27918870
35828449
84810153

Do you want to disallow multiple uses of the same authentication token? This restricts you to one login about every 30s, but it increases your chances to notice or even prevent man-in-the-middle attacks (y/n) y

By default, a new token is generated every 30 seconds by the mobile app. In order to compensate for possible time-skew between the client and the server, we allow an extra token before and after the current time. This allows for a time skew of up to 30 seconds between authentication server and client. If you experience problems with poor time synchronization, you can increase the window from its default size of 3 permitted codes (one previous code, the current code, the next code) to 17 permitted codes (the 8 previous codes, the current code, and the 8 next codes). This will permit for a time skew of up to 4 minutes between client and server.

Do you want to do so? (y/n) y

If the computer that you are logging into isn't hardened against brute-force login attempts, you can enable rate-limiting for the authentication module. By default, this limits attackers to no more than 3 login attempts every 30s. Do you want to enable rate-limiting? (y/n) y

www.stefanbaur.de@cloudshell:~\$

Befehlsfenster

Einrichtung SSH+2FA (Teil 5)

- Die Scratch Codes sollte man sich nun ausdrucken und z.B. in den Tresor oder die Geldbörse packen.
- Danach geht es mit folgenden Fragen und Antworten weiter:
 - Do you want me to update your
"/home/userle/.google_authenticator" file? (y/n) y
 - Do you want to disallow multiple uses of the same authentication token? This restricts you to one login about every 30s, but it increases your chances to notice or even prevent man-in-the-middle attacks (y/n) y

Einrichtung SSH+2FA (Teil 6)

- Danach geht es mit dieser Frage weiter – ich empfehle „y“, außer man ist völlig paranoid:

- By default, a new token is generated every 30 seconds by the mobile app.

In order to compensate for possible time-skew between the client and the server, we allow an extra token before and after the current time. This allows for a time skew of up to 30 seconds between authentication server and client. If you experience problems with poor time synchronization, you can increase the window from its default size of 3 permitted codes (one previous code, the current code, the next code) to 17 permitted codes (the 8 previous codes, the current code, and the 8 next codes). This will permit for a time skew of up to 4 minutes between client and server.

Do you want to do so? (y/n) y

Einrichtung SSH+2FA (Teil 7)

- Und zuletzt noch:
 - If the computer that you are logging into isn't hardened against brute-force login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting? (y/n) y

The background is a solid blue color. At the top, there are three stylized, light blue clouds. In the center, there is a bright, glowing sun. At the bottom, there is a decorative border consisting of a series of small, light blue, pointed shapes.

Zusatzinfos

Was wir heute *nicht* gezeigt haben

Möglich, aber heute aus Zeitgründen nicht im Vortrag (kommerzieller Support bei Bedarf verfügbar, siehe Folie mit Support-Kontaktdaten) wären folgende Zusatzfunktionen:

- Virtualisierung (zwecks einfacherem Failover)
- Einbindung in LDAP-/Active-Directory-Infrastruktur
- High Availability (HA) mit Heartbeat
- WiFi (auch als Gastnetz, ggf. mit Captive Portal, ...)
- Nutzung der LEDs zur Anzeige verschiedener Betriebszustände
- Portabler X2GoClient (USB-Stick mit ThinClient-Image und Windows-Client)

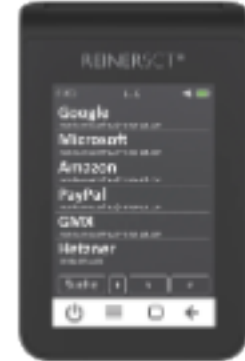
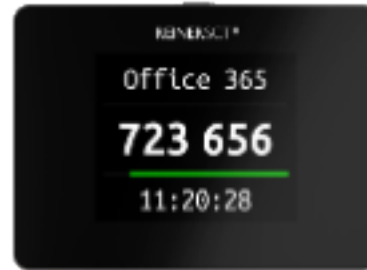
X2GoClient – sogar auf USB-Stick

- X2GoClient braucht keine Adminrechte
- Doppelinstallation möglich:
 - Windows-X2GoClient als Portable Application
 - vom Stick bootfähige X2Go-ThinClientEdition
 - Kernel, Ramdisk, Squashfs, Syslinux und Windows-X2GoClient kommen in ein FAT-Dateisystem

Windows XP im Jahr 2024 – es lebt!

- Top 4 der im Jahr 2024 noch produktiv genutzten Windows-XP-Systeme:
 - Geldautomaten
 - Medizingeräte
 - Kassensysteme
 - Industrielle Steuerungs- und Automatisierungssysteme (ICS)
- Quelle: <https://www.howtogeek.com/things-you-wont-believe-still-run-windows-xp/>

Hardware-TOTP-Generatoren



- Alternative, wenn
 - kein Smartphone gewünscht/verfügbar ist
 - TOTP-gesicherte Logins auch vom Smartphone aus erfolgen sollen, wo womöglich auch noch der Passwortmanager installiert ist:
Zweiter Faktor und Passwort auf selbem Gerät gespeichert?
→ Das ist kein zweiter Faktor mehr!
- Kombigeräte können TOTP und Online-Banking-TANs generieren

Kosten für CM4-basierte Lösung



Raspberry Pi CM4 (2 GB RAM, 8 GB Flash, kein WiFi/BT)	42,10 Euro
Setpreis BaseBoard + Gehäuse + Netzteil	68,95 Euro
Porto	11,90 Euro
Gesamt	122,95 Euro

(Alle Preise brutto und vom 20.03.2025, CM4 bei Reichelt, restliches Set Eckstein)