

Handout WLAN-SG für Linux-Geräte

Version 1.8

Voraussetzung:

1. Die mobilen Endgeräte müssen schuleigene Geräte sein und von der Schule administriert werden, um Zertifikate aufspielen zu dürfen.
2. Diese Endgeräte werden im pädagogischen Netz eingesetzt.
3. Die SSID (WLAN-SG) wird ausgestrahlt.
 - Unter den verfügbaren WLAN-Netzen wird "WLAN-SG" angezeigt.
4. Das mobile Gerät hat einen eindeutigen Namen.
5. Die Zertifikatsdateien (**Passwortgeschützt**) liegen vor und sind zugänglich.
6. Das Passwort für die Zertifikatsdatei ist identisch mit dem per E-Mail zugesandten Passwort für das Herunterladen der Zertifikate.
7. Bei der Installation der Zertifikate können Sie wählen, ob Zertifikate **mehrfach (schulbasiertes Zertifikat)** oder für **jedes Endgerät** ein eigenes Zertifikat (**gerätebasiertes Zertifikat**) verwendet werden soll.
 - **Gerätebasiertes Zertifikat:**
 - Auf jedem Endgerät wird eigenes Zertifikat installiert und nicht mehrfach verwendet.
 - **Schulbasiertes Zertifikat:**
 - Ihnen werden standardmäßig eine geplante Anzahl an Zertifikaten zur Verfügung gestellt, damit jedes Gerät mit einem eigenen Zertifikat ausgestattet werden kann. Sie können aber auch ein einziges Ihrer Zertifikate für alle Geräte oder einen Teil der Geräte einer Schule oder eines Standortes verwenden. (Schulbasiertes Zertifikat)
8. Es wird dringend empfohlen, eine Liste zu führen welches Gerät (Gerätename und MAC Adresse) welches Zertifikat erhalten hat, um diese später zurückziehen oder erneuern zu können.
 - Wenn ein Gerät abhandenkommt kann ein gerätebasiertes/schulbasiertes Zertifikat zurückgezogen (revoked) werden, um z. B. die unbefugte Verwendung der Verbindung zu verhindern (bei Verlust oder Diebstahl).
 - Wenn ein Zertifikat zurückgezogen werden muss, teilen Sie uns den zugehörigen Namen des Zertifikats mit."
9. Für die Installation verfügen Sie über Root-Rechte.

Handout WLAN-SG für Linux-Geräte

Version 1.8

Vorbereitung

- 1) Laden Sie zunächst die beiden Ordner mit den Zertifikaten auf einen USB-Stick herunter. Ihnen stehen zwei Ordner zur Verfügung:
 - Der Ordner mit Ihrer Schulnummer und Namen der Schule (Bsp.: 1234-Gymnasium Musterschule) beinhaltet Ihre Zertifikate.
 - Im Ordner "Handout + WLAN-Profil" finden Sie das benötigte WLAN-Profil für die WLAN-SSID "WLAN-SG".
- 2) Entpacken Sie die beiden heruntergeladenen Ordner auf den USB-Stick.

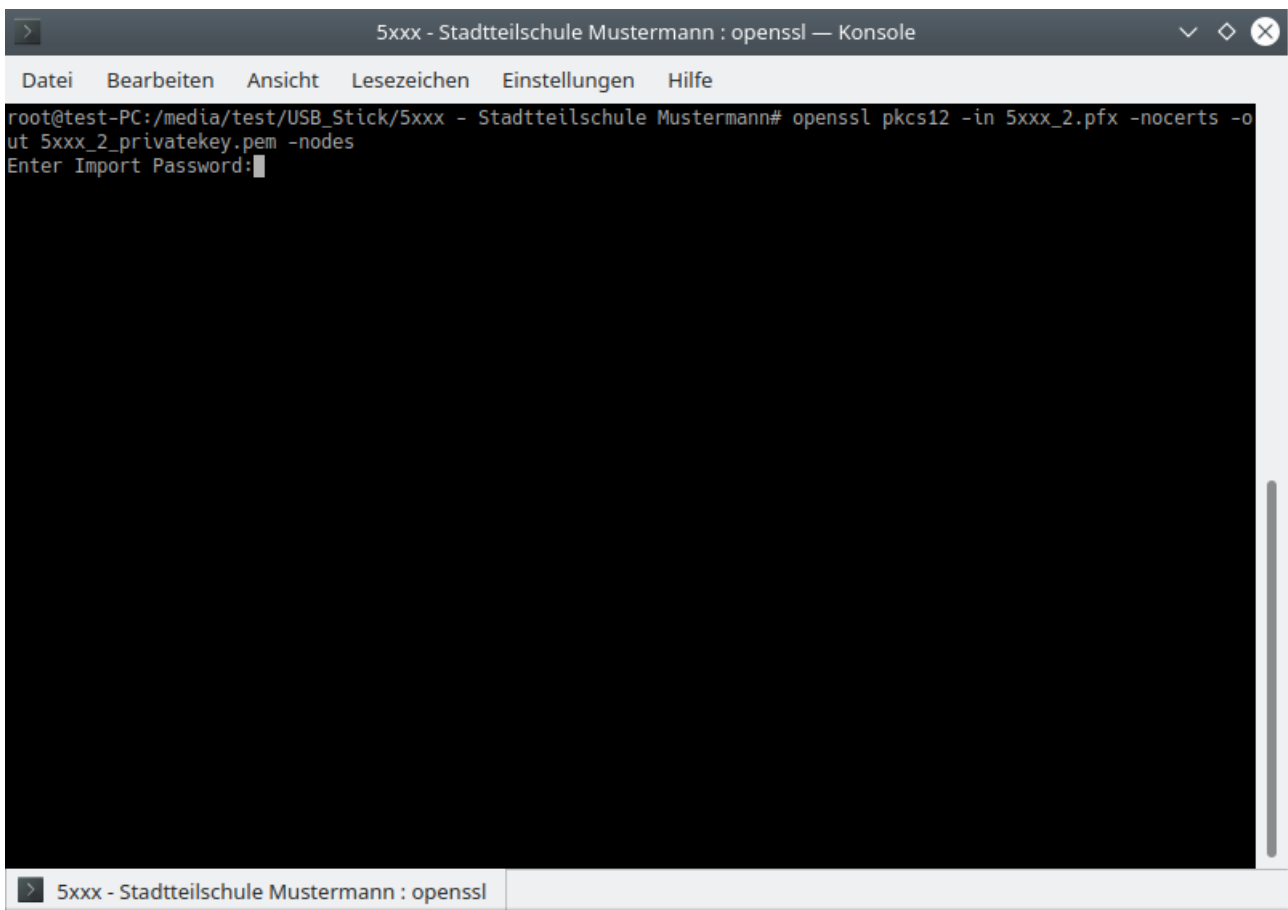
Wenn Sie sich für gerätbasiertes Zertifikat (jedes Endgerät ein eigenes Zertifikat) entscheiden, **wird es dringend empfohlen, jedes bereits benutzte Zertifikat eindeutig umzubenennen oder zu löschen, um nicht versehentlich ein Zertifikat doppelt zu installieren.**

Handout WLAN-SG für Linux-Geräte

Version 1.8

Exportieren des Private-Keys aus der pfx-Datei

1. Für das Ausführen der Befehle sind Root-Rechte notwendig.
2. **Zuerst trennen Sie bitte unbedingt alle Verbindungen im WLAN.** Wenn das Gerät vorher mit „hamburg-schule“ verbunden war, um das Zertifikat herunterzuladen, soll die Verbindung vorher getrennt und am besten alle gespeicherten Credentials zu hamburg-schule (WLAN-Anmeldeinformationen: Benutzername und Passwort) gelöscht werden.
3. Schließen Sie den USB-Stick mit den Zertifikatdateien an das mobile Endgerät an.
4. Wechseln Sie zum Verzeichnis mit dem WLAN-Zertifikat. (Als Beispiel in diesem Abschnitt: [5xxx – Stadteilschule Mustermann](#))
5. Geben Sie folgenden Befehl für ein **unbenutztes Zertifikat** im Linux-Terminal ein:
 - `openssl pkcs12 -in 5_xxx_2.pfx -nocerts -out 5_xxx_2_privatekey.pem -nodes`
 - Als Beispiel in diesem Abschnitt: [5xxx_2.pfx](#)
6. Geben Sie Ihr Zertifikat-Passwort bei Abfrage ein.
 - Das Passwort für die Zertifikatsdatei ist identisch mit dem per E-Mail zugesandten Passwort für das Herunterladen der Zertifikate.



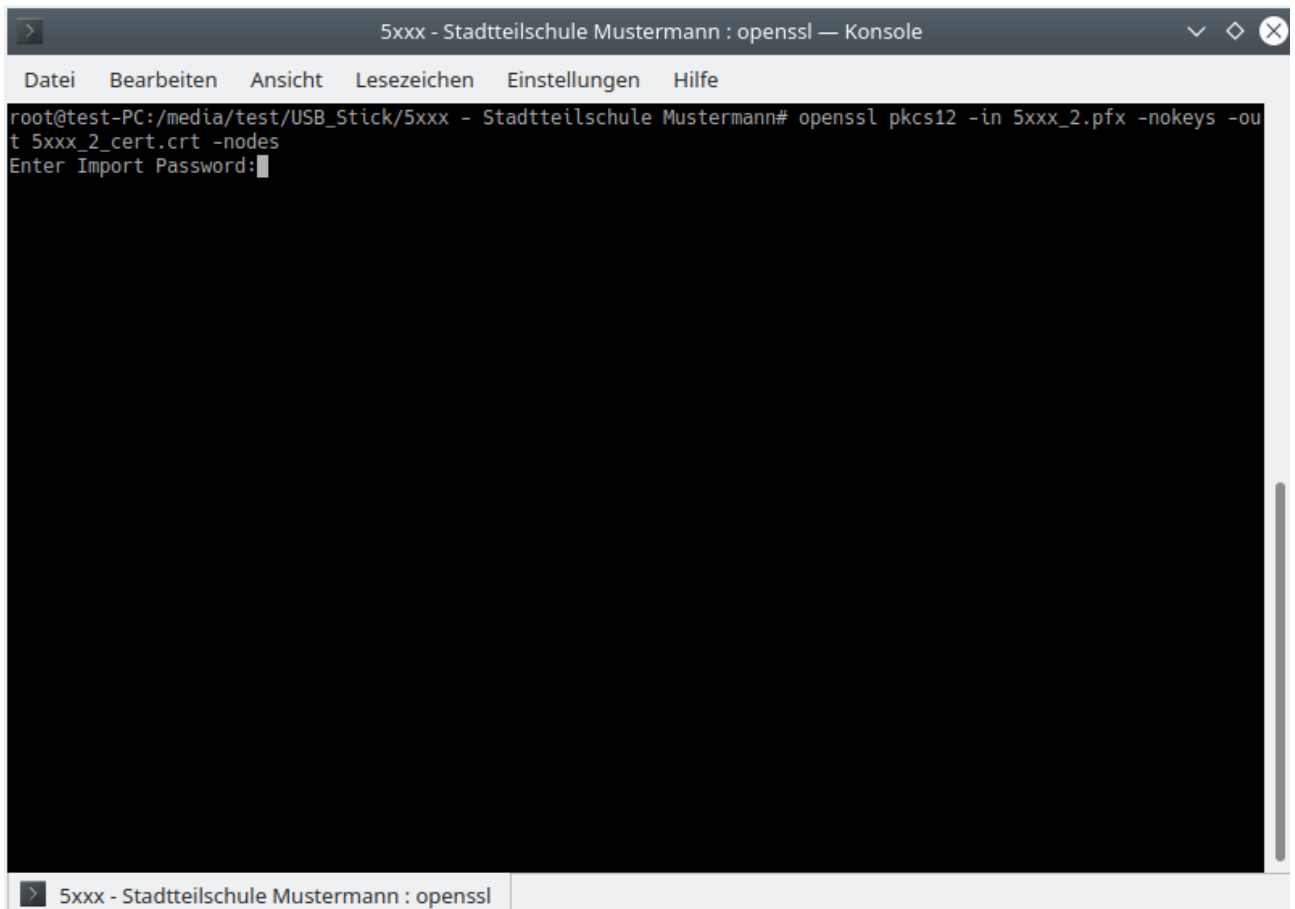
```
5xxx - Stadteilschule Mustermann : openssl — Konsole
Datei Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe
root@test-PC:/media/test/USB_Stick/5xxx - Stadteilschule Mustermann# openssl pkcs12 -in 5xxx_2.pfx -nocerts -o
ut 5xxx_2_privatekey.pem -nodes
Enter Import Password:
```

Handout WLAN-SG für Linux-Geräte

Version 1.8

Exportieren des Zertifikats aus der pfx-Datei

1. Für das Ausführen der Befehle sind Root-Rechte notwendig.
2. Geben Sie folgenden Befehl für ein **unbenutztes Zertifikat** im Linux-Terminal ein:
 - `openssl pkcs12 -in 5_xxx_2.pfx -nokeys -out 5_xxx_2_cert.crt -nodes`
 - Als Beispiel in diesem Abschnitt: `5xxx_2.pfx`
3. Geben sie ihr Zertifikat-Passwort bei Abfrage ein.
 - Das Passwort für die Zertifikatsdatei ist identisch mit dem per E-Mail zugesandten Passwort für das Herunterladen der Zertifikate.



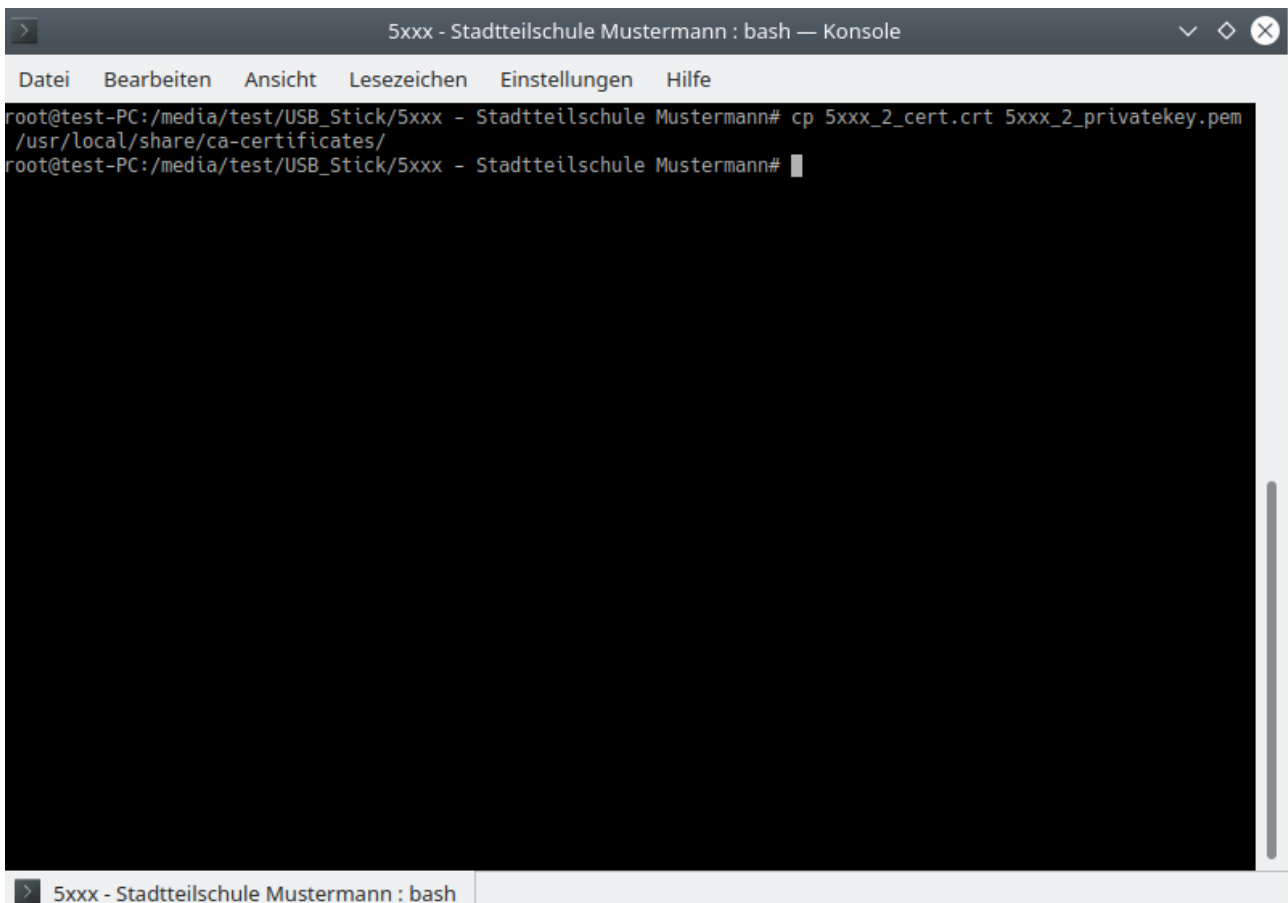
```
5xxx - Stadtteilschule Mustermann : openssl — Konsole
Datei Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe
root@test-PC:/media/test/USB_Stick/5xxx - Stadtteilschule Mustermann# openssl pkcs12 -in 5xxx_2.pfx -nokeys -out
5xxx_2_cert.crt -nodes
Enter Import Password:
```

Handout WLAN-SG für Linux-Geräte

Version 1.8

Kopieren der Zertifikatsdateien auf den Rechner

1. Kopieren Sie bitte die erzeugte Private-Key und das Zertifikat auf den Rechner, der das WLAN-Zertifikat erhalten soll.
 - Zielordner: `/usr/local/share/ca-certificates/`
2. Geben Sie dafür folgenden Befehl im Linux-Terminal ein:
 - `cp 5xxx_2_cert.crt 5xxx_2_privatekey.pem /usr/local/share/ca-certificates/`
 - Als Beispiel in diesem Abschnitt: `5xxx_2_cer.crt` und `5xxx_2_privatekey.pem`



The image shows a terminal window titled "5xxx - Stadtteilschule Mustermann : bash — Konsole". The terminal content is as follows:

```
root@test-PC:/media/test/USB_Stick/5xxx - Stadtteilschule Mustermann# cp 5xxx_2_cert.crt 5xxx_2_privatekey.pem /usr/local/share/ca-certificates/
root@test-PC:/media/test/USB_Stick/5xxx - Stadtteilschule Mustermann#
```

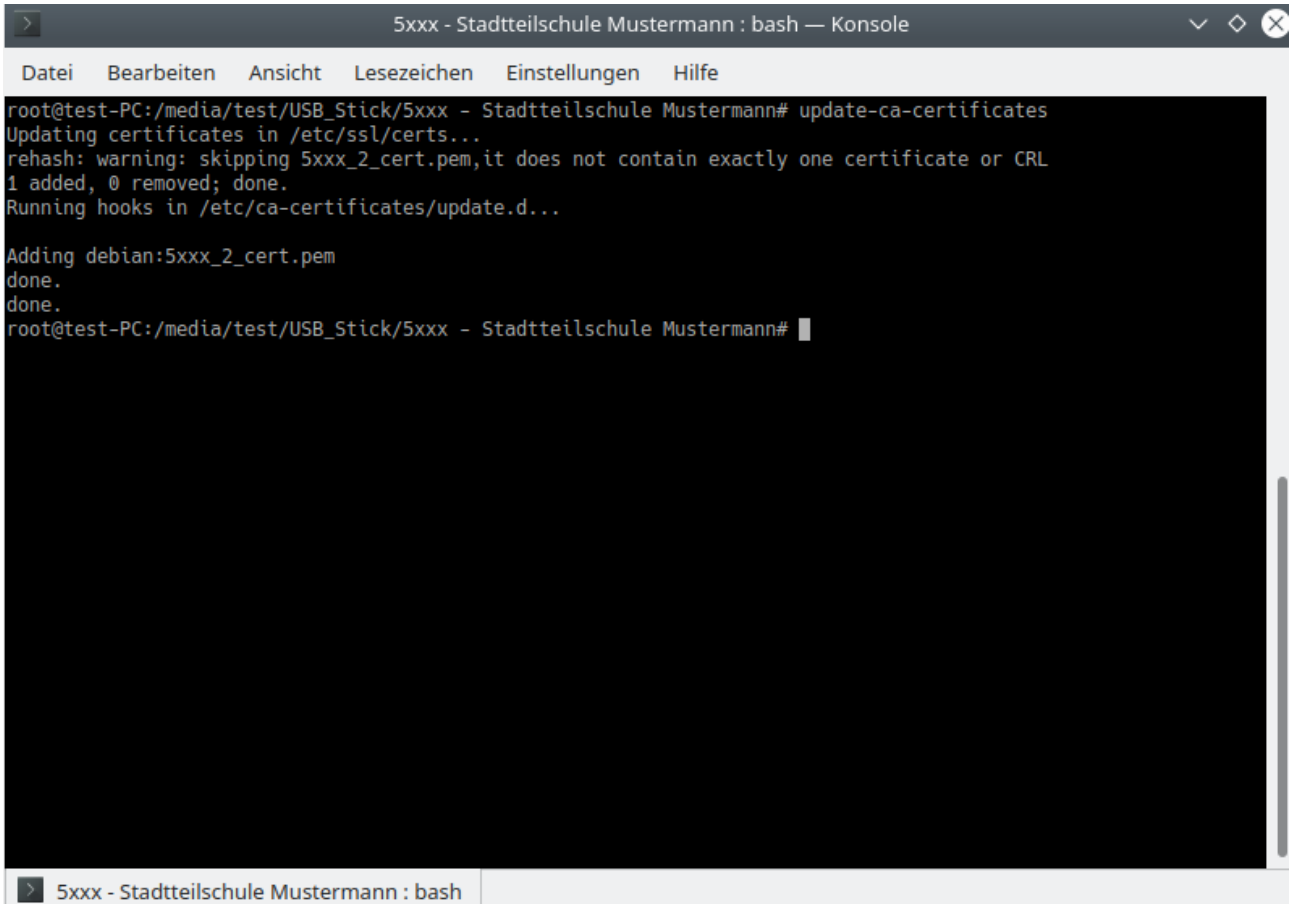
Handout WLAN-SG für Linux-Geräte

Version 1.8

Update des Zertifikatsverzeichnis

1. Geben Sie folgenden Befehl im Linux-Terminal ein:

- `update-ca-certificates`



```
5xxx - Stadteilschule Mustermann : bash — Konsole
Datei Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe
root@test-PC:/media/test/USB_Stick/5xxx - Stadteilschule Mustermann# update-ca-certificates
Updating certificates in /etc/ssl/certs...
rehash: warning: skipping 5xxx_2_cert.pem, it does not contain exactly one certificate or CRL
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...

Adding debian:5xxx_2_cert.pem
done.
done.
root@test-PC:/media/test/USB_Stick/5xxx - Stadteilschule Mustermann#
```

Handout WLAN-SG für Linux-Geräte

Version 1.8

Stellen Sie eine Verbindung mit dem "WLAN-SG" her.

1. Nach dem Erscheinen des Anmeldefensters wählen Sie folgende Einstellungen aus (orientiert an Xubuntu-18 Oberfläche):

- 1.1. Sicherheit des Funknetzwerks: [WPA-& WPA2-Enterprise Legitimierung: TLS](#)
- 1.2. Identität: [WLAN-SG](#)
- 1.3. CA-Zertifikat: [/pfad/zu/5xxx_xx_cert.crt](#)
 - 1.3.1. Als Beispiel in diesem Abschnitt: [/usr/local/share/ca-certificates/5xxx_2_cert.crt](#)
- 1.4. User-Zertifikat: [/pfad/zu/5xxx_xx_cert.crt](#)
 - 1.4.1. Als Beispiel in diesem Abschnitt: [/usr/local/share/ca-certificates/5xxx_2_cert.crt](#)
- 1.5. Geheimer User-Schlüssel: [/pfad/zu/5xxx_xx_privatekey.pem](#)
 - 1.5.1. Als Beispiel in diesem Abschnitt: [/usr/local/share/ca-certificates/5xxx_2_privatekey.pem](#)

2. Auf "Verbindung" klicken.

Installation ist abgeschlossen!

Das Gerät ist nun mit dem WLAN-SG verbunden.

Hinweise:

Für den Fall, dass es zu Problemen kommt, kann dies an fehlenden Rechten des eingeloggten Benutzers liegen.

Lösungsansatz:

Ändern sie den Besitzer der .pem und .crt auf den Benutzer, mit dem die Verbindung erstellt wird:

- `chown <user>:<group> <dateiname>`

Alternativ, falls der NetworkManager verwendet wird, führen Sie den nm-connection-editor mit root-Rechten aus:

- `sudo nm-connection-editor`

Legen Sie eine neue Funknetzwerk-Verbindung an. Unter SSID tragen Sie "WLAN-SG" ein und unter Gerät wählen Sie das Funkgerät des Computers. Als Verbindungsnamen tragen Sie einen beliebigen Namen ein und tragen unter dem Reiter "Sicherheit des Funknetzwerks" alle Einstellungen wie im Abschnitt „Stellen Sie eine Verbindung mit dem „WLAN-SG“ her“ ein.