



Keyway

WHITEPAPER · VERSION 1.0 · OKTOBER 2026

Sicherer Fernzugriff im Browser für IT und OT

Architektur, Sicherheitsmodell und Betrieb eines selbst gehosteten Web-Clients für SSH, VNC und SFTP – vom Serverraum bis zum Schaltschrank.



Keyway 0.3.0 · MIT-Lizenz
keyway.iotueli.com/de/

Zusammenfassung

Keyway ist ein selbst gehosteter Web-Client, der SSH-Terminal, Fernbildschirm (VNC), Dateiverwaltung (SFTP), einen verschlüsselten Tresor für Zugangsdaten und eine Offline-Befehlshilfe in einem Browser-Tab vereint. Er läuft als ein kleiner Container auf deiner eigenen Hardware – ohne Cloud-Dienst und ohne Konto bei Dritten – und funktioniert am Rechner, auf dem Tablet und auf dem Telefon.

Wer Server, SPS, HMI-Panels, Gateways und Raspberry Pis betreut, jongliert meist mit mehreren Programmen: SSH-Client, VNC-Viewer, SFTP-Client und einer Passwortliste. Keyway ersetzt diese Werkzeugkette durch eine einheitliche Oberfläche, die ein Funkloch übersteht, Passwörter und Schlüssel verschlüsselt auf dem Server hält und keinen offenen VNC-Port im Anlagennetz braucht.

1 Container

linux/amd64 und
linux/arm64

4 Werkzeuge

Terminal, Bildschirm,
Dateien, Befehlshilfe

AES-256-GCM

Tresor, Schlüssel per
Argon2id

MIT

Open Source, kostenlos

Das Wichtigste

- Ein Browser-Tab für SSH, VNC und SFTP auf jedem Gerät, auch am Telefon mit Tastenleiste und Gesten.
- VNC läuft standardmässig durch SSH: Der Bildschirm reist verschlüsselt, der VNC-Server kann nur auf localhost lauschen.
- Zugangsdaten liegen verschlüsselt; der Tresor-Schlüssel existiert nur im Speicher und verschwindet beim Sperren.
- Gehärtet: keine Shell im Image, unprivilegierter Nutzer, schreibgeschütztes Dateisystem, keine Linux-Capabilities.
- Für das eigene Netz gebaut. Von aussen nur über VPN oder einen Reverse-Proxy mit eigenem Zertifikat.

Inhalt

01 Das Problem mit dem Fernzugriff

02 Was Keyway ist

03 Architektur

04 Funktionen im Detail

05 Sicherheitsmodell

06 Betrieb in IT- und OT-Netzen

07 Backup, Updates, Wiederherstellung

08 Einsatzszenarien

09 Loslegen

Das Problem mit dem Fernzugriff

Moderne Standorte mischen klassische IT und Betriebstechnik: Linux-Server und virtuelle Maschinen neben SPS, HMI-Panels, IoT-Gateways, Wallboxen, Wechselrichtern und Einplatinenrechnern. Jede Geräteklasse bringt gern ihren eigenen Zugangsweg mit.

- **Werkzeug-Wildwuchs.** SSH-Client, VNC-Viewer, SFTP-Client und eine Notizdatei mit Adressen – auf jedem Laptop installiert, der Zugriff braucht, und selten auf dem Telefon.
- **Verstreute Zugangsdaten.** Passwörter und private Schlüssel liegen in lokalen Client-Profilen, Textdateien oder Browser-Passwortmanagern, oft ohne zentrale Verschlüsselung und ohne sauberen Weg, sie zu wechseln.
- **Offene VNC-Ports.** Panels und HMIs bieten VNC oft auf Port 5900 im ganzen Netz an, geschützt nur durch die schwache VNC-Passwortabfrage.
- **Brüchige Sitzungen.** Ein abgerissenes WLAN oder Mobilnetz beendet einen langen Befehl oder eine offene Editor-Sitzung.
- **Wissenslücken.** Servicetechniker sind nicht immer Linux-Profis. Den richtigen Befehl samt Schaltern zu finden kostet Zeit – und auf Anlagen ohne Internet gibt es keine schnelle Suche.

Keyway löst diese Probleme mit einem einzigen, selbst gehosteten Zugangspunkt, den das Team über den Browser erreicht.

Was Keyway ist

Keyway ist ein selbst gehosteter Web-SSH- und VNC-Client mit SFTP, verschlüsseltem Tresor und Offline-Befehlshilfe. Man kann es sich wie eine komplette Terminal-Suite vorstellen – nur im Browser und auf der eigenen Hardware. Die Oberfläche gibt es auf Deutsch und Englisch; sie folgt der Sprache des Browsers.

Eigenschaft	Wert
Aktuelle Version	0.3.0 (Oktober 2026)
Lizenz	MIT (Namen und Logos «Keyway» und «IoTUeli» sind Marken und nicht erfasst)
Auslieferung	Container-Image <code>iotuelich/keyway</code> (Docker Hub) und <code>ghcr.io/uiff/keyway</code>
Plattformen	linux/amd64, linux/arm64 (z. B. Raspberry Pi, Industrie-PC)
Technik	Go-Backend, eingebettete Weboberfläche, SQLite, Terminal mit <code>xterm.js</code> , Bildschirm mit <code>noVNC</code>
Protokolle zu Geräten	SSH (Terminal, SFTP, Port-Weiterleitung für VNC), VNC/RFB 3.3, 3.7, 3.8
Zugang für Nutzer	HTTPS in jedem aktuellen Browser auf Rechner, Tablet und Telefon; auf dem Startbildschirm installierbar
Sprachen	Deutsch, Englisch
Quellcode	<code>github.com/uiff/ssh-app</code>

Architektur

Keyway ist ein einzelnes Go-Programm in einem einzelnen Container. Der Browser spricht über HTTPS und zwei WebSocket-Endpunkte mit ihm (Terminal unter `/api/ws`, Bildschirm unter `/api/vnc`). Alle Verbindungen zu den Geräten gehen vom Keyway-Server aus, nie vom Browser.

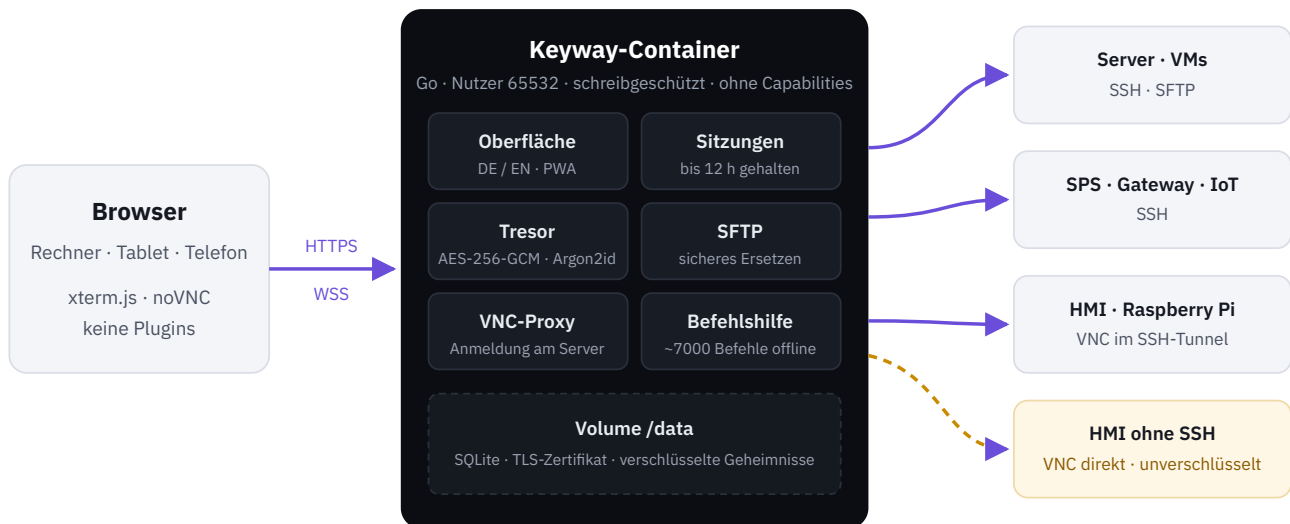


Abbildung 1 – Architektur. Alle Verbindungen zu Geräten starten beim Keyway-Server; der Browser erhält nur Terminalausgabe und Bildschirminhalt.

Datenfluss

1. Die Anmeldung läuft über HTTPS. Aus dem Anmeldepasswort wird zugleich der Schlüssel abgeleitet, der den Tresor öffnet (Argon2id).
2. Beim Öffnen eines Hosts entschlüsselt Keyway den gespeicherten Zugang im Speicher, verbindet sich per SSH und prüft den Host-Schlüssel.
3. Terminaldaten fließen über den WebSocket `/api/ws`. Die SSH-Sitzung läuft bis zu 12 Stunden auf dem Server weiter und hängt sich nach einem Neuladen oder Funkloch wieder an.
4. Für den Bildschirm meldet sich Keyway selbst am VNC-Server an und reicht nur Bild und Eingaben an den Browser weiter (`/api/vnc`). Standardmässig läuft VNC per SSH-Port-Weiterleitung zu `127.0.0.1:<port>` auf dem Gerät.
5. Dateien laufen per SFTP über dieselbe SSH-Verbindung; Uploads landen zuerst in einer temporären Datei und werden dann eingesetzt.

Funktionen im Detail

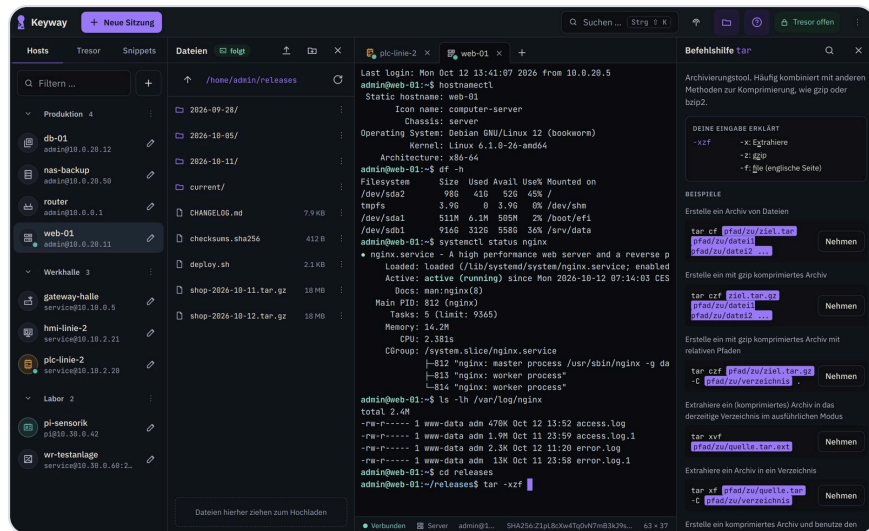


Abbildung 2 – Arbeitsplatz: Hosts in Ordnern, Dateileiste folgt dem Terminal, SSH-Sitzung und Befehlshilfe zu `tar -xzf`.

Terminal

- Tabs, 256 Farben, Vollbildprogramme (top, htop, vi), anklickbare Links, Kopieren und Einfügen.
- Sitzungen überstehen Neuladen und Funklöcher bis zu 12 Stunden.
- Verständliche Fehler statt Netzwerk-Codes; Abbruch nach rund 20 Sekunden.
- Host-Schlüssel bestätigen beim ersten Verbinden, deutliche Warnung bei Änderung.
- An alle senden: Eingaben gleichzeitig an mehrere Sitzungen.
- Kritische Hosts: Rückfrage vor `rm -rf`, `dd` oder `reboot` aus Snippets, Hilfe oder «An alle senden».

Dateien (SFTP)

- Hochladen (auch per Ziehen), Herunterladen, Umbenennen, Löschen, Ordner anlegen.
- Sicheres Ersetzen erhält Besitzer, Rechte, Hardlinks und Bind-Mounts.
- Die Dateileiste folgt `cd` im Terminal auf Linux-Hosts.

Hosts, Tresor und Backup

Jeder Host hat einen Gerätetyp mit Symbol – SPS, HMI/Panel, Gateway, IoT-Gerät, Wallbox, Wechselrichter, Server, VM, Container, PC, Raspberry Pi, Router, Switch, Firewall, NAS, Cloud/VPS oder Drucker – dazu Ordner, Tags, Farben und Notizen. Das Adressfeld versteht `user@host:port`, `ssh://...` und ganze `ssh -p` Befehlszeilen. Zugänge lassen sich von mehreren Hosts gemeinsam nutzen; ed25519-Schlüssel erzeugt Keyway

Bildschirm (VNC)

- Bildschirme öffnen als Tabs neben den Terminals, auch mehrere gleichzeitig.
- Über SSH getunnelt (Vorgabe) oder direkt für Panels ohne SSH.
- Ansicht und Zoom, Qualitätsstufen, Nur ansehen, Zwischenablage, Sondertasten inklusive Strg+Alt+Entf und F1–F12.
- Touch: Tippen klickt, langes Drücken klickt rechts, zwei Finger scrollen, Spreizen zoomt, Tastenleiste.
- Geräteschlüssel (RSA-AES-Anmeldung) werden gemerkt und wie SSH-Host-Schlüssel geprüft.

Befehlshilfe und Suche

- Rund 7000 Befehle aus den tldr-pages, offline, auf Deutsch und Englisch.
- Erklärt die Schalter des Befehls in der aktuellen Zeile.
- Suche in Alltagssprache («archiv entpacken»), Snippets mit Platzhaltern, eine Suche für Hosts, Snippets und Befehle.

auf Knopfdruck und hinterlegt sie auf dem Host. Ein einziges verschlüsseltes Backup enthält Hosts, Ordner, Zugänge, Snippets und bekannte Host-Schlüssel.

Sicherheitsmodell

Keyway ist ein Gateway, das Zugangsdaten für viele Geräte hält. Das Sicherheitsmodell schützt deshalb vor allem gespeicherte Geheimnisse, begrenzt, was ein Browser erreichen kann, und härtet den Container selbst.

Bereich	Massnahme
Gespeicherte Geheimnisse	Passwörter und private Schlüssel liegen nur verschlüsselt vor (AES-256-GCM). Der Schlüssel wird per Argon2id aus dem Anmeldepasswort abgeleitet, lebt nur im Speicher und verschwindet beim Sperren des Tresors.
Sitzungsdauer	Automatische Abmeldung und Tresor-Sperre nach 30 Minuten ohne Bedienung (einstellbar). Laufende Terminal-Sitzungen laufen weiter.
Anmeldeschutz	15 Minuten Sperre nach 5 Fehlversuchen pro Adresse (IPv6 je /64). HttpOnly- und SameSite=Strict-Cookies, eigener Header gegen CSRF, strenge Content Security Policy.
Namensprüfung	Schutz vor DNS-Rebinding im HTTP-Modus und sobald erlaubte Namen gesetzt sind; WebSockets nur, wenn Origin und Host passen.
Zielkontrolle	Keyway verbindet sich nur mit Adresse und Port, die beim Host gespeichert sind – der Browser kann kein anderes Ziel nennen.
Geräte-Identität	SSH-Host-Schlüssel und VNC-Geräteschlüssel (RSA-AES) werden beim ersten Mal bestätigt und danach bei jeder Verbindung geprüft.
VNC-Geheimnisse	Das VNC-Passwort bleibt auf dem Server; Keyway meldet sich selbst an. Nach 5 falschen Passwörtern wird die Verbindung geschlossen.
Gefährliche Befehle	Hosts mit dem Tag <code>kritisch</code> verlangen eine Bestätigung für zerstörerische Befehle aus Snippets, Hilfe oder «An alle senden».
Container	Keine Shell im Image, unprivilegierter Nutzer 65532; die Compose-Datei setzt ein schreibgeschütztes Dateisystem, entfernt alle Capabilities und setzt no-new-privileges.
Lieferkette	Images baut GitHub Actions aus dem öffentlichen Repository, testet und startet sie vor der Veröffentlichung und versieht sie mit Provenance-Nachweis und SBOM.

Bekannte Grenzen – offen gesagt

- Zum Verbinden muss der Server ein Geheimnis kurz entschlüsseln. Ende-zu-Ende-Verschlüsselung bis in den Browser ist bei einem SSH-Gateway nicht möglich. Kopien der Go-Laufzeit lassen sich nicht zuverlässig löschen; wer den Prozessspeicher lesen kann (root, Core-Dump, Swap), kann sie finden.
- Im Modus *direkt* ist der VNC-Verkehr zwischen Keyway und Gerät unverschlüsselt und nur durch die schwache VNC-Abfrage geschützt. Nur in vertrauenswürdigen Netzen nutzen.
- Bis das erste Konto angelegt ist, kann jeder, der die Adresse erreicht, Keyway einrichten. Die Einrichtung direkt nach dem ersten Start abschliessen.
- Keyway ist für das eigene Netz gedacht und gehört nicht ungeschützt ins Internet.

Betrieb in IT- und OT-Netzen

Keyway läuft überall, wo Docker läuft. Die Compose-Datei aus dem Repository setzt die beschriebene Härtung bereits um.

```
mkdir keyway && cd keyway
curl -fsSL0 https://raw.githubusercontent.com/uiff/ssh-app/main/compose.yml
docker compose up -d
# danach https://<adresse>:8443 öffnen und sofort einrichten
```

Hinter einem Reverse-Proxy

Für ein vertrauenswürdigen Zertifikat läuft Keyway im HTTP-Modus hinter Caddy, nginx oder Traefik. Der Proxy muss WebSockets durchreichen, den Host-Header unverändert weitergeben (oder `X-Forwarded-Host` setzen), `X-Forwarded-For` setzen und grosse Uploads erlauben.

Variable	Zweck
<code>SSHAPP_TLS=aus</code>	Nur HTTP, ausschliesslich hinter einem Reverse-Proxy (<code>auto</code> = selbst signiert, <code>eigen</code> = eigenes Zertifikat)
<code>SSHAPP_COOKIE_SECURE=1</code>	Sitzungs-Cookie nur über HTTPS senden
<code>SSHAPP_PROXY</code>	Vertrauenswürdige Proxys; Anmeldesperre pro Browser über X-Forwarded-For
<code>SSHAPP_HOSTS</code>	Erlaubte Namen (Schutz vor DNS-Rebinding)
<code>SSHAPP_LEERLAUF_MIN</code>	Minuten ohne Bedienung bis zur Abmeldung (Vorgabe 30)

Platzierung in Industrienetzen

In Anlagen, die in Zonen und Conduits gegliedert sind (zum Beispiel nach IEC 62443), passt Keyway als kontrollierter Zugangspunkt in eine Wartungs- oder Managementzone. Empfehlungen:

- Keyway in dem Netzsegment betreiben, das die Zielgeräte erreichen darf – nicht am Internet-Rand.
- Von aussen nur über VPN oder einen authentifizierenden Reverse-Proxy erreichbar machen; dort Mehr-Faktor-Anmeldung ergänzen.
- Für VNC «Über SSH getunnelt» bevorzugen, damit Panels VNC nur auf localhost anbieten und die Firewall Port 5900 nicht öffnen muss.
- Produktionskritische Hosts als `kritisch` markieren und je Gerätegruppe eigene Zugänge im Tresor führen.
- Vor jedem Update ein Backup herunterladen und den Sicherheitsschlüssel getrennt aufbewahren, etwa im Passwortmanager.

Eine praxisnahe Einführung in Zonen, Conduits und Netzsegmentierung in OT-Umgebungen gibt es kostenlos unter ot.iotueli.com.

Backup, Updates, Wiederherstellung

Backup und Umzug

Einstellungen > Backup lädt eine verschlüsselte Datei herunter. Auf einem neuen System beim ersten Start «Backup wiederherstellen» wählen und Datei und Sicherheitsschlüssel angeben. Passwörter und Schlüssel bleiben im Backup verschlüsselt.

Sicherheitsschlüssel

Der Sicherheitsschlüssel erscheint bei der Einrichtung genau einmal. Er setzt ein vergessenes Passwort zurück und öffnet Backups – ohne ihn ist ein Backup nicht lesbar.

Updates

Backup herunterladen, dann `docker compose pull` und `docker compose up -d`. Tags: `latest`, eine genaue Version wie `0.3.0` oder eine Versionslinie wie `0.3` (nur Fehlerbehebungen).

Dein Sicherheitsschlüssel

Damit setzt du das Passwort zurück und spielst ein Backup auf einem anderen System ein. Er wird nur jetzt angezeigt – ohne ihn sind Backups nicht lesbar.

G5QU-PQNV-04YX-YKT3-MZIL-H4WR-
JWRL-D7FI-NGH2-CBMF-QGNG-USLV-
2BSA

Kopieren

Als Datei speichern

⚠ Bewahre ihn getrennt von Keyway auf, zum Beispiel in deinem Passwort-Manager.

☐ Ich habe den Sicherheitsschlüssel sicher aufbewahrt.

Weiter zu Keyway

Abbildung 3 – Der Sicherheitsschlüssel wird bei der Einrichtung nur einmal angezeigt.

Einsatzszenarien

Instandhaltung in der Industrie

Servicetechniker öffnen die Shell des SPS-Gateways, prüfen Logs, kopieren eine Konfigurationsdatei und sehen sich den HMI-Bildschirm von Linie 2 an – alles in einem Tab am Laptop vor dem Schaltschrank, ohne Software auf Kundengeräten zu installieren.

Aussendienst am Telefon

Vor Ort oder im Pikett stehen dieselben Hosts und Bildschirme auf dem Telefon bereit, mit Tastenleiste für Esc, Tab, Strg und Pfeile und Gesten für den Fernbildschirm.

IoT- und Edge-Flotten

Raspberry Pis, Gateways und Edge-Geräte sind in Ordnern mit Gerätetyp und Tags organisiert. «An alle senden» führt denselben Befehl auf mehreren Geräten aus.

Homelab und kleine IT

Ein Container auf NAS oder Mini-PC gibt Haushalt oder Büro einen zentralen, verschlüsselten Ort für SSH- und VNC-Zugriffe.

Loslegen

1. **Starten:** Container mit Docker Compose hochfahren (siehe Kapitel 06).
2. **Sofort einrichten:** Benutzer und ein Passwort mit mindestens 10 Zeichen wählen, Sicherheitsschlüssel sicher ablegen.
3. **Hosts hinzufügen:** Gerätetyp wählen, Adresse und Benutzer eintragen, verbinden.
4. **Bildschirm einschalten** für HMI-Panels unter Erweitert > Bildschirm (VNC), über SSH getunnelt.

Weiterführend

Produktseite: keyway.iotueli.com/de/
 Quellcode und Dokumentation:
github.com/uiff/ssh-app
 Container-Images:
hub.docker.com/r/iotuelich/keyway ·
ghcr.io/uiff/keyway
 Lernseite OT-Security: ot.iotueli.com

```

pi@pi-sensorik:~$ systemctl is-active sensor
active
pi@pi-sensorik:~$ vcgencmd measure_temp
temp=47.2'C
pi@pi-sensorik:~$ df -h /
Filesystem      Size  Used Avail Use% Mounted on
/dev/mmcblk0p2  29G   6.8G   21G   25% /
pi@pi-sensorik:~$ cd messung
pi@pi-sensorik:~/messung$ ls
2026-10-10.csv  2026-10-11.csv  2026-10-12.csv
pi@pi-sensorik:~/messung$ tail -n 24 *12.csv
2026-10-12T13:33:00,21.2,48.8,1012.9
2026-10-12T13:34:00,21.2,48.8,1012.8
2026-10-12T13:35:00,21.3,48.6,1012.8
2026-10-12T13:36:00,21.2,48.7,1012.8
2026-10-12T13:37:00,21.2,48.7,1012.7
2026-10-12T13:38:00,21.3,48.6,1012.8
2026-10-12T13:39:00,21.4,48.5,1012.8
2026-10-12T13:40:00,21.4,48.5,1012.7
2026-10-12T13:41:00,21.5,48.3,1012.7
2026-10-12T13:42:00,21.4,48.4,1012.7
2026-10-12T13:43:00,21.4,48.4,1012.6
2026-10-12T13:44:00,21.5,48.3,1012.7
2026-10-12T13:45:00,21.6,48.2,1012.7
2026-10-12T13:46:00,21.6,48.2,1012.6
2026-10-12T13:47:00,21.7,48.0,1012.6
2026-10-12T13:48:00,21.6,48.1,1012.6
2026-10-12T13:49:00,21.6,48.1,1012.5
2026-10-12T13:50:00,21.7,48.0,1012.6
2026-10-12T13:51:00,21.8,47.9,1012.6
2026-10-12T13:52:00,21.8,47.9,1012.5
2026-10-12T13:53:00,21.9,47.7,1012.5
2026-10-12T13:54:00,21.8,47.8,1012.5
2026-10-12T13:55:00,21.8,47.8,1012.4
2026-10-12T13:56:00,21.9,47.7,1012.5
pi@pi-sensorik:~/messung$

```

Abbildung 4 – Terminal auf dem Telefon.

Über IoTUeli

Keyway wird von IoTUeli entwickelt und als Open Source veröffentlicht. Mehr über IoTUeli unter iotueli.com.

© 2026 IoTUeli. Keyway steht unter der MIT-Lizenz. «Keyway» und «IoTUeli» sind Marken von IoTUeli und fallen nicht unter die MIT-Lizenz. Befehlshilfe aus den tldr-pages (CC BY 4.0); Fernbildschirm mit noVNC (MPL-2.0). Stand Oktober 2026, Version 0.3.0. Das Titelbild ist mit KI erstellt; die gezeigten Oberflächen sind echte Bildschirmfotos von Keyway.