dormakaba

Terminal ONE / Terminal 96 00

Technisches Handbuch

04500551 - 07/2024

DE

Inhaltsverzeichnis

1 Zu diesem Dokument

1.1 Gültigkeit

Dieses Dokument beschreibt das Produkt:

Produktbezeichnung:	Terminal 96 00	Terminal ONE
Produktkennung:	9600-K7	ONE-K7
Artikelnummer:	04579602	04579610
Gerätesoftware:	772-00-X-K00	
BaseApp:	796-00-X-K00	
Testprogramm:	739-00-X-K00	
Herstellungsdatum:	Ab April 2024	

Dieses Dokument beschreibt alle Produktvarianten und alle optionalen Ausstattungen und Funktionen. Optionen sind kostenpflichtig und daher nur verfügbar, wenn sie erworben wurden. Zusatz-Ausstattungen und -Funktionen können zum Zeitpunkt der Dokumentausgabe noch nicht verfügbar sein und möglicherweise erst zu einem späteren Zeitpunkt erworben werden.

1.2 Zielgruppe

Dieses Dokument richtet sich ausschließlich an Fachkräfte.

1.3 Inhalt und Zweck

Der Inhalt beschränkt sich auf die Montage, Installation, Inbetriebnahme und die grundsätzliche Bedienung des Produktes.

1.4 Warnhinweise

Warnhinweise mit Angaben bzw. Ge- und Verboten zur Verhütung von Personen- und Sachschäden sind besonders gekennzeichnet.

Warnhinweise bitte beachten! Sie sollen helfen, Unfälle zu verhüten und Schäden zu vermeiden.

1.4.1 Gefahrenkategorien

Warnhinweise sind in folgende Kategorien eingeteilt:

⚠ VORSICHT

Geringes Risiko

Bezeichnet eine möglicherweise gefährliche Situation, die zu leichten Körperverletzungen führen kann.

ACHTUNG

Hinweise für den sachgerechten Umgang mit dem Produkt.

Das Nichtbeachten dieser Hinweise kann zu Fehlfunktionen führen. Das Produkt kann beschädigt werden.

1.4.2 Symbole

Je nach Gefahrenquelle werden für Warnhinweise Symbole mit folgender Bedeutung verwendet.

Gefahr allgemein

Gefahr für elektronische Komponenten durch elektrostatische Entladung

1.5 Hinweise

Hinweise sind mit einem Info-Symbol gekennzeichnet.

Anwendungstipps, nützliche Informationen
Diese Tipps helfen, das Produkt und dessen Funktionen optimal zu nutzen.

1.6 Handlungsanweisungen

Der Aufbau und die Symbolik der Handlungsanweisungen ist in folgendem Beispiel verdeutlicht:

✓ Voraussetzung

1. Handlungsschritt 1
   ⇨ Zwischenergebnis
2. Handlungsschritt 2

⇨ Ergebnis

2 Grundlegende Sicherheitshinweise

Dieses Dokument lesen und beachten, bevor das Gerät verwendet wird, um Personen- und Sachschäden zu vermeiden.

2.1 Bestimmungsgemäße Verwendung

Dieses Gerät ist bestimmt für den Einsatz als Endgerät zur Eingabe und Anzeige von Daten der Zeiterfassung, Türsteuerung und Mitarbeiterkommunikation.

Eine sonstige Verwendung ist nicht bestimmungsgemäß.

2.2 Qualifikation der Personen

Die in diesem Dokument beschriebenen Handlungen müssen von Fachkräften ausgeführt werden. Die Fachkräfte müssen von dormakaba geschult und autorisiert sein.

Fachkräfte haben eine geeignete technische Ausbildung und Erfahrung mit der verwendeten Technik. Fachkräfte sind für die Einhaltung der vom Hersteller genannten Bedingungen sowie geltende Vorschriften und Normen verantwortlich.

2.3 Lithium-Batterie

Das Gerät enthält 1 Lithium-Batterie des Typ CR2032 als Stützbatterie.

- Die Batterie benötigt keine Service- oder Wartungsarbeiten. Die Haltbarkeit der Batterie ist bis zum Ende des Lebenszyklus ausgelegt.
- Die Sicherheitsvorschriften für den Transport von Geräten mit Lithium-Batterie einhalten.

2.4 Montage und Installation

- Durch Transport/falsche Lagerung kann das Gerät beschädigt sein.
  - Das Gerät auf sichtbare Schäden prüfen.
  - Kein beschädigtes Gerät in Betrieb nehmen.
- Der Installationsort muss die klimatischen und technischen Bedingungen des Herstellers erfüllen.

2.5 Zubehör und Ersatzteile

- Nur die von dormakaba freigegebenen Komponenten und Bauteile verwenden.
- Die elektrischen Vorgaben (Spannung/Leistungsaufnahme) einhalten.

2.6 Service und Wartung

- Umbauten und Veränderungen am Gerät sind nicht zulässig.

2.7 Datenschutz und IT-Sicherheit

Das Gerät muss für einen sicheren Betrieb konfiguriert werden.

Ohne weitere Sicherheitseinstellungen kann unbefugt auf das Gerät und das System zugegriffen werden.

Sicherheitsrisiken

- Verletzung des Datenschutzes durch unberechtigten Zugriff auf personenbezogene Daten.
- Unberechtigter Zutritt
- Sabotage/Systemausfall

Empfohlene Maßnahmen

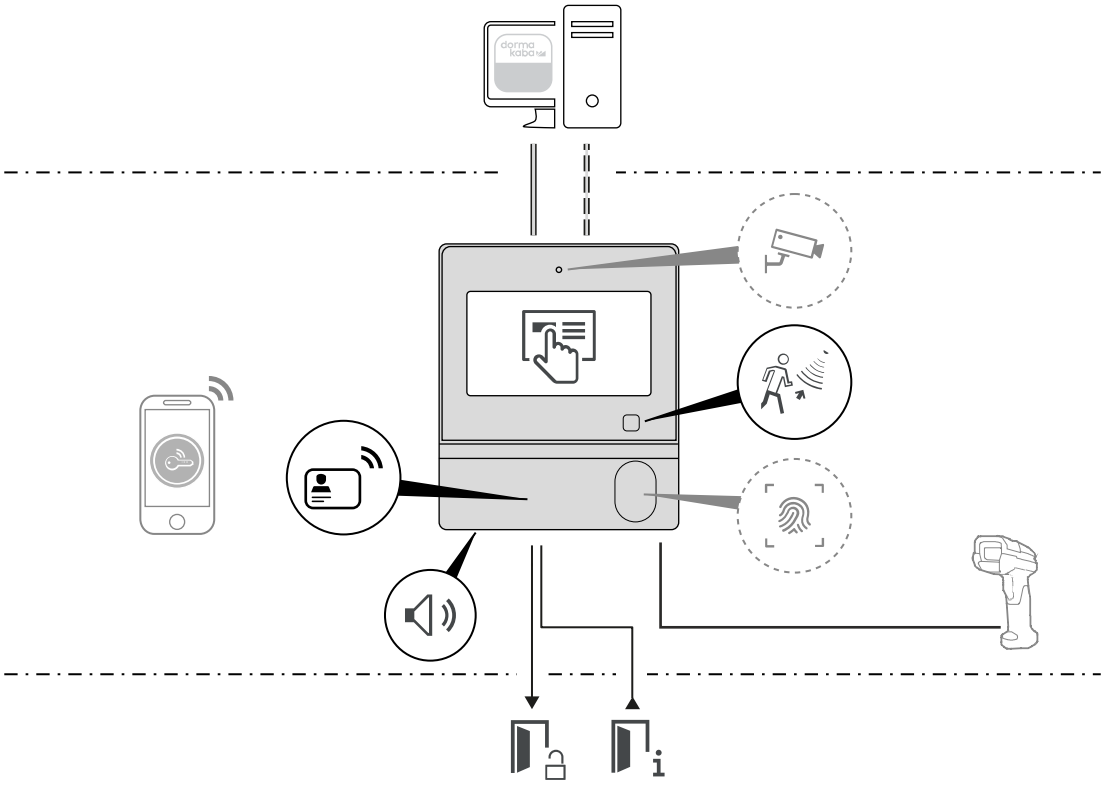
- Gerät/Service Interface:
  - Werkseitige Terminal-Passwort ändern.
  - Werkseitige Service-Interface-Passwort ändern.
  - Gerätesoftware aktuell halten.
  - Werkseitige SSH-Schlüsseldatei gegen kundenspezifische SSH-Schlüsseldatei tauschen.
  - SSH-Server nach Inbetriebnahme/Wartung deaktivieren.
  - Web-Server nach Inbetriebnahme/Wartung deaktivieren.
  - Vor Außerbetriebnahme: Das Gerät auf die Werkeinstellung zurücksetzen.
- Browser (Verbindung mit Service Interface):
  - Passwörter nicht im Browser speichern.
  - Während der Verbindung mit dem Service Interface, im Browser keine weiteren Webseiten öffnen.
  - Vor dem Schliessen des Browsers, vom Service Interface abmelden.
  - Vor dem Schliessen des Browsers, den Browser-Verlauf löschen.
- Systemsoftware:
  - Verschlüsselte Kommunikation aktivieren.
  - Aktuelle Patches einspielen.

Die empfohlenen Maßnahmen beziehen sich nur auf das Gerät, ohne Anspruch auf Vollständigkeit und Aktualität.

Der Betreiber des Systems muss durch geeignete Maßnahmen den Schutz von personenbezogener Daten und der IT-Sicherheit in seiner gesamten Organisation sicherstellen.

3 Produktbeschreibung

3.1 Übersicht



Mit dem Terminal können Daten für die Zeiterfassung und Mitarbeiterkommunikation mittels RFID oder Biometrie erfasst werden. Die Interaktion mit dem Benutzer findet über den Touchscreen statt. Eine Verwendung als Türsteuerung für 1 Tür ist möglich.

Die Identifizierung der Benutzer erfolgt abhängig von der Konfiguration mit:

- RFID-Medium

  Die Funktionen CardLink, AoC und DoC zum Schreiben von Daten auf RFID-Medien werden unterstützt.
- Smartphone mit Mobile Access App via Bluetooth®/NFC (Option)
- Fingerabdruck-Leser (Option)

Die übergeordnete Systemsoftware verwaltet das System. Die Kommunikation zwischen dem Gerät und der Systemsoftware erfolgt wahlweise über:

- LAN
- WLAN

Um den Energieverbrauch zu reduzieren, geht das Terminal bei Nichtbenutzung nach einiger Zeit in den Standby-Modus. Die Akivierung erfolgt über einen Näherungssensor.

Optional ist eine Kamera integriert.

Ein Lautsprecher gibt akkustische Rückmeldungen.

Das Gerät hat für die Türsteuerung 1 Ausgang und 2 Eingänge. Über den Ausgang kann ein Zutrittskontrollstellglied angesteuert werden. Türzustände können über die Eingänge erfasst werden.

An den USB-Anschluss kann optional ein weiteres Gerät, wie z.B. ein Barcodescanner, angeschlossen werden.

3.2 Technische Daten

3.2.1 System

Betriebssystem

- Android 12

CPU

- i.MX8M Mini Quad Processor

Speicher

- 4 GByte DDR4 RAM
- 16 GByte eMMC Flash

Display

- Typ: TFT
- Größe: 5.0"
- Auflösung: 1280 x 720 Pixel (16:9 diagonal)
- Kontrast: 1200:1, typisch 800:1
- Helligkeit: 430-500 cd/m²
- Beleuchtung: LED
- Touchpanel: kapazitiv

Audio

- Integrierter Lautsprecher (1 W)

3.2.2 Stromversorgung

PoE gemäß IEEE802.3af (12,96 W)

3.2.3 Schnittstellen

- Ethernet: 10/100/1.000 Mbit/s
- USB: 2.0, Buchse Typ C

3.2.4 Frequenzbänder und Sendeleistung

- WLAN:
  - 2,4 GHz (IEEE 802.11 b/g/n), max. 200 mW, 23 dBm
  - 5 GHz (IEEE 802.11 a/h/j/n/ac), max. 200 mW, 23 dBm
- RFID: 13,56 MHz
  - LEGIC: max. 345 mW
  - HID: max. 1000 mW
- Bluetooth: max. 2,5 mW

3.2.5 Eingänge (IN1-IN2)

- Zum Anschluss potentialfreier Kontakte
- Integrierte Spannungsversorgung: 5 V DC

3.2.6 Ausgang (OUT)

- 1 Wechselkontakt
- Kontaktbelastbarkeit: 30 V AC/DC; max. 2 A

3.2.7 Leser

Je nach Ausführung werden folgende Leser unterstützt:

RFID-Leser

- RFID-Chip: SM 6300
- Leseverfahren:
  - LEGIC advant, ISO 14443A
  - MIFARE DESFire, ISO 14443A
  - OSS-SO Version 2021-06
  - HID - iCLASS SE
  - HID - iCLASS, Prox, Prox II
  - Mobile Access (Bluetooth Low Enegery/NFC)

Fingerabdruck-Leser

- Biometric Module (CBM) mit integrierter Datenbank für Fingerabdrücke.
- Optional als CBM-E mit erweiterten Zulassungen (PIV-IQS mit FBI Zertifizierung und FIPS 201 zugelassene Template Auswertung)
- Speicherkapazität
  - ONE: 1.000 Stammsätze
  - 96 00: 50.000 Stammsätze

3.2.8 Umgebungsbedingungen

Schutzart nach IEC 60529

- IP20
- IP65, wenn Installationsvorgaben eingehalten werden.

Relative Feuchtigkeit

- 5% - 85%, nicht kondensierend

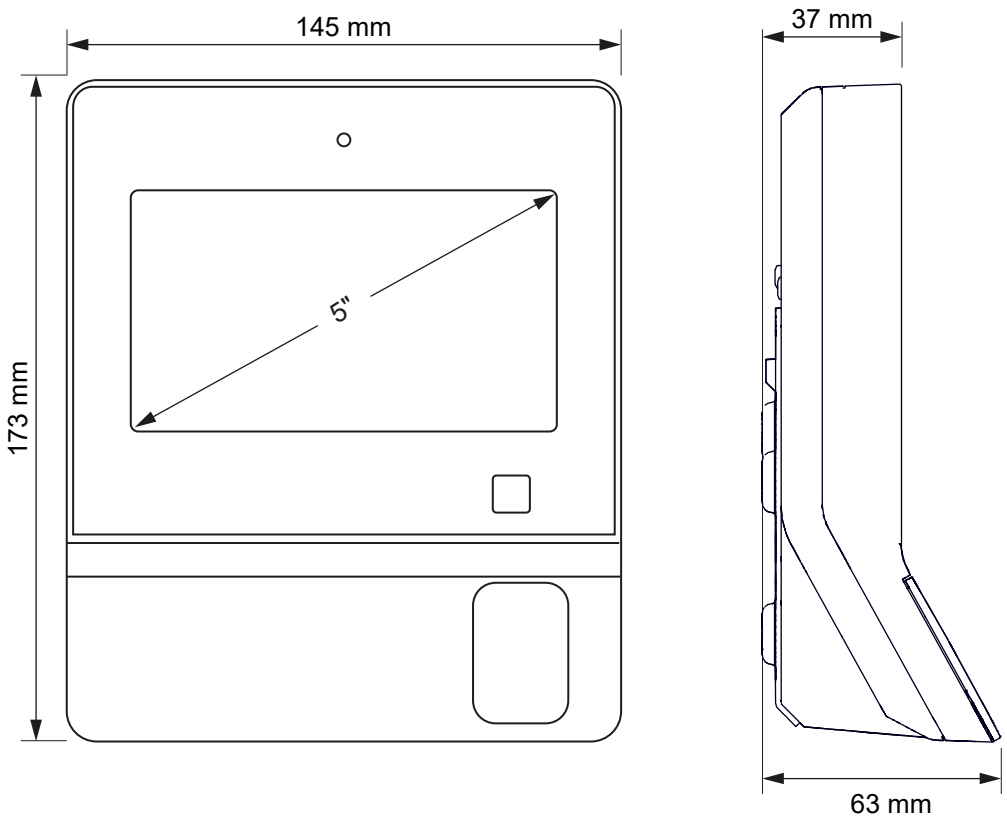
Umgebungstemperatur
Umweltklasse 3K6:

- -25 °C – +55 °C (Betrieb)
- -20 °C – +70 °C (Lager)

Stoßfestigkeit

- IK06

3.2.9 Abmessungen



3.3 Konformität

Dieses Produkt entspricht den Bestimmungen der EU-Richtlinien:

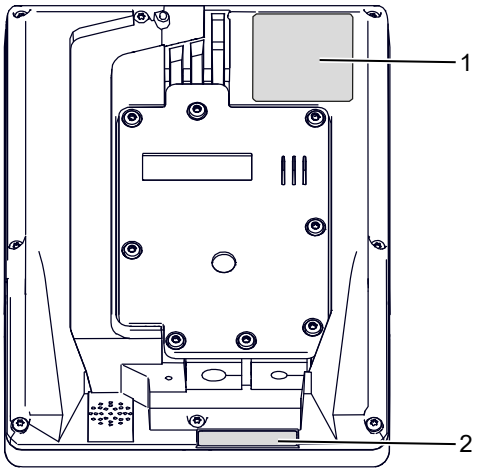
- **2011/65/EU - Restriction of Hazardous Substances (RoHS)**
- **2014/53/EU - Radio Equipment Directive (RED)**

Vollständige Konformitätserklärungen sind online verfügbar.

https://techdoc.dormakaba.com/cds/go/9600-K7

3.4 Kennzeichnung

Die Produktkennzeichnung befindet sich auf der Rückseite des Terminals.



1 Typenschild mit folgenden Inhalt
   - Produktbezeichnung
   - Artikelnummer
   - Herstellungsdatum
   - Daten zur Stromversorgung
   - Verschiedene Symbole (Konformität, Sicherheit, Entsorgung)

2 Seriennummer

3.5 Lieferumfang

- Terminal
- Montageplatte
- Für Befestigung an die Wand:
  - Schraube 4,5 x 35 (3 Stück)
  - Dübel (3 Stück)
- Zum Abdichten der Leitungseinführungen
  - Kabeltülle 6 (1 Stück)
  - Kabeltüllenstopfen 6 (1 Stück)
  - Kabeltülle 8 (1 Stück)
  - Kabeltüllenstopfen 8 (1 Stück)

3.6 Zubehör

3.6.1 Dichtungs-Set IP65

Um die Schutzart IP65 zu erreichen, werden zusätzliche Teile benötigt.

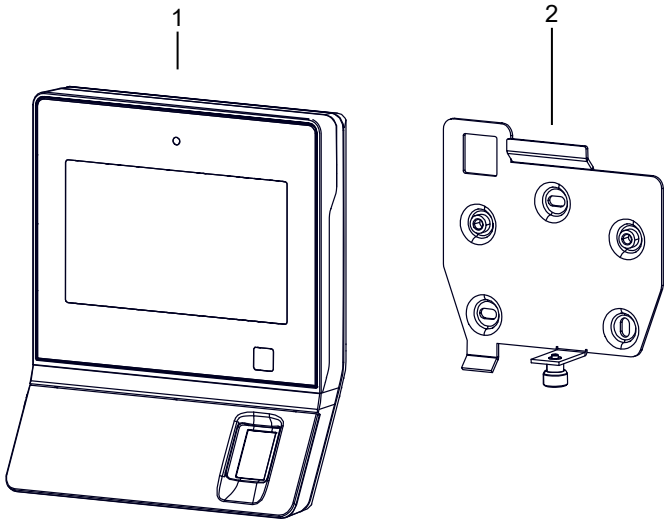
- Kabelabdeckung IP65
  - 8 Schrauben
- Kabeltüllen
  - Kabeltülle 5 (1 Stück)
  - Kabeltülle 7 (1 Stück)
  - Kabeltülle 9 (1 Stück)
  - Blindtülle BTK (1 Stück)

Bestellnummer: 04500555 (DE, VIS)

4 Aufbau und Funktion

4.1 Bestandteile

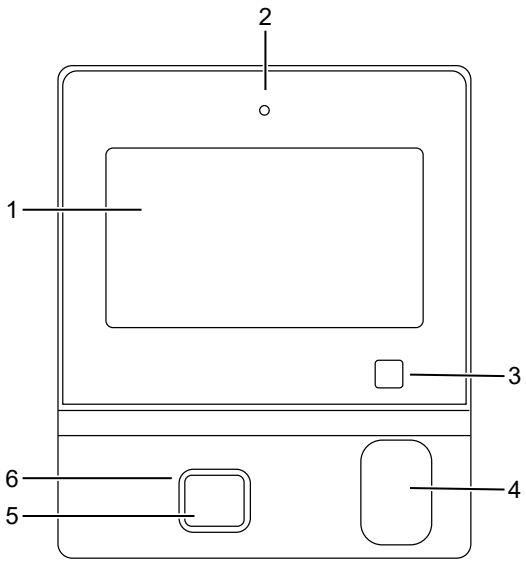
Das Terminal hat einen Bewegungssensor zur Sabotageerkennung. Wird das Terminal im Betrieb bewegt, erzeugt die Gerätesoftware ein Alarmsatz.



1 Terminal

2 Montageplatte

4.2 Vorderseite



1 Touchscreen

2 Kamera (Option)

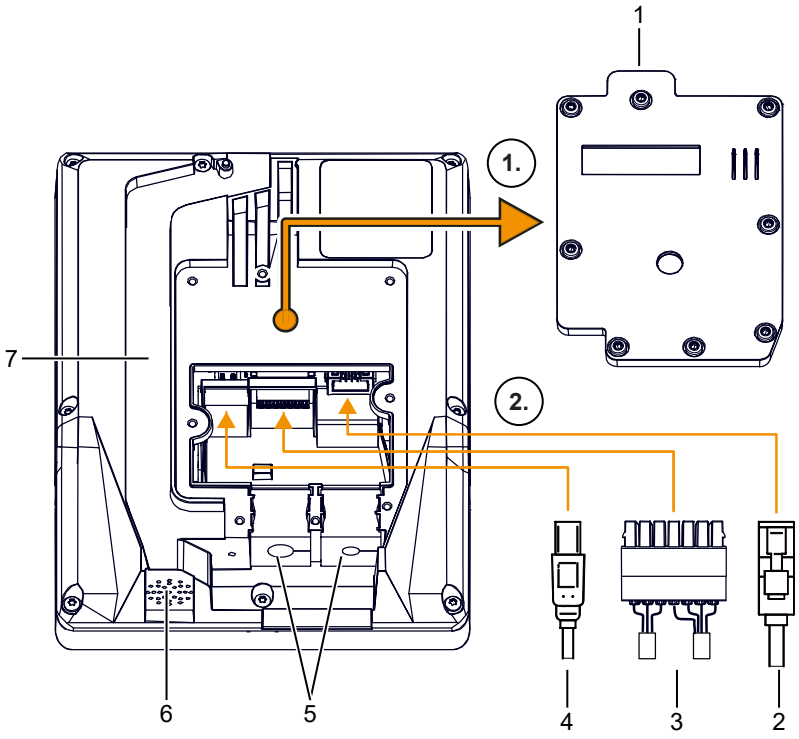
3 Näherungssensor

4 Fingerabdruckleser (Option)

5 RFID-Leser

6 Leuchtring RFID-Leser

4.3 Rückseite



1	Kabelabdeckung IP20	2	LAN-Buchse (RJ45)
3	Anschlussklemmen für Eingänge/Ausgang	4	USB-Buchse (Typ C)
5	Kabeltüllen	6	Lautsprecher
7	Kabelkanal zur Leitungsführung von oben nach unten		

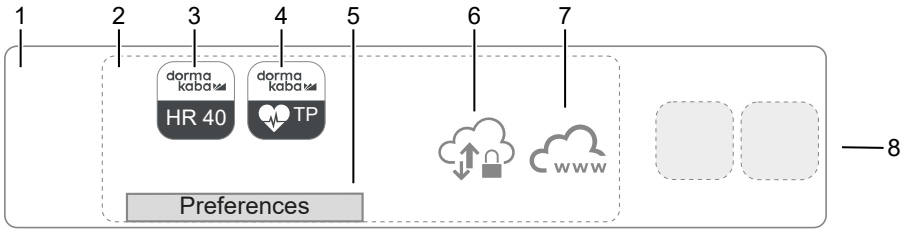
4.4 Varianten

Ausstattung	ONE	96 00		
		96 20	96 40	96 60
Gerätesoftware				
B-Client HR40	●	●	●	●
Leser				
RFID-Leser, LEGIC / MIFARE (SM6300)	●	●	●	●
HID iClass SE / Prox	○	○	○	○
Fingerabdruckleser	○	○	○	○
Schnittstelle (Host)				
Ethernet 10/100/1.000 (PoE)	●	●	●	●
WLAN	○	○	○	○
Anwendungen				
Mobile Access	–	●	●	●
CardLink / Access on Card (AoC)	–	–	●	●
Türsteuerung	○	–	–	●
Lautsprecher	●	●	●	●
Energiesparmodus mit Näherungssensor	●	●	●	●
Kamera	–	●	●	●
Speicher				
1.000 Stammsätze	●	–	–	–
50.000 Stammsätze	–	●	●	●

Legende

● standard ○ optional – nein

4.5 Übersicht Gerätesoftware



1 Betriebssystem Android

2 **BaseApp**

Die BaseApp gehört zur Grundausstattung und ist die Plattform für alle Apps auf dem Terminal.

Wichtige Funktionen der BaseApp:

- Schützen des Betriebssystems vor unberechtigtem Zugriff.
- Organisieren und Starten der Apps.
- Bereitstellen von Funktionen und Schnittstellen für den Zugriff auf die Hardware.
- Bereitstellen von Service-Funktionen zur Inbetriebnahme und Wartung des Gerätes.

3 **B-Client HR40**

Übernimmt die Funktionen für Zeiterfassung und Türsteuerung.

Details siehe Referenzhandbuch B-Client HR40

4 **Testprogramm**

Systemeinstellungen: Konfigurieren der Leser, Service-Sprache

Tests: Leser, Display, Touchscreen, Ein- und Ausgänge, Sensoren

Anzeigen von Informationen über das Terminal

5 Preferences, je nach Aufruf

- **Service Interface** – lokal

  Bietet Funktionen zur Inbetriebnahme, dem Betrieb und der Wartung.

- **Android-Systemeinstellungen**

  Bietet Funktionen zur Inbetriebnahme, dem Betrieb und der Wartung.

6 **SSH-Server**

- Ermöglicht einen Fernzugriff mit einem SFTP-Client.
  Auf das Dateiensystem des Terminals kann direkt zugegriffen werden.
- Ermöglicht einen Fernzugriff auf das Terminal mit einem SSH-Client.
  Mittels Befehle können Service-Funktionen ausgeführt werden.

7 **Web-Server**

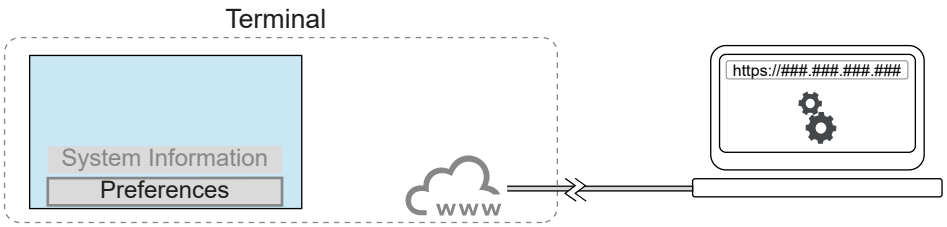
Ermöglicht einen Fernzugriff auf das Service Interface mit einem Browser.

8 Optionale Apps

Es können weitere Apps installiert werden, wenn zusätzliche Funktionen benötigt werden.

4.5.1 Service Interface

Funktionen für die Inbetriebnahme, den Betrieb und für die Wartung sind über das Service Interface des Terminals verfügbar.



Es gibt 2 Möglichkeiten das Service Interface aufzurufen.

- Lokal, über den Touchscreen des Terminals
- Fernzugriff, über den Browser eines Rechners

Eine Anmeldung mit Benutzername (admin) und Service-Interface-Passwort ist notwendig.

Es gibt 3 Bereiche.

1 System

- Informationen
  Aktuelle Informationen über Hardware, Gerätesoftware, MAC-Adresse und IP-Adresse
- Lizenz
  Aktuelle Informationen über die lizensierten Funktionen.
- Diagnose
  Protokolldateien können angezeigt und heruntergeladen werden.
- Administration
  Funktionen: reboot device (Neustart), disable Serviceinterface (Web-Server abschalten), cold restart (Gerät wird auf Werkseinstellungen zurück gesetzt), SSH-Schlüssel zurücksetzen

2 Einstellungen

- Netzwerk
- Biometrie
- Datum und Uhrzeit
- Benutzerverwaltung
- Anzeigeverwaltung
- HR-Client

3 Firmware

- Firmware-Download

  Die Firmware des internen RFID-Lesers kann aktualisiert werden.

5 Installation

5.1 Installationsbedingungen

5.1.1 Installationsort

- Gerät ortsfest in Gebäuden installieren. Die Installation in Fahrzeugen ist nicht zulässig.
- Gerät nur an Orten installieren, die mit den Umgebungsbedingungen des Geräts übereinstimmen.

Elektromagnetische Störungen vermeiden

- Gerät nicht im Bereich starker elektromagnetischer Felder installieren. (Mögliche Störquellen: Schaltnetzteile, Starkstromleitungen, ...)

Funkstörungen vermeiden

- Zu weiteren RFID-Leser einen Abstand von mindestens 20 cm einhalten.
- Zu weiteren Mobile Access Komponenten (Bluetooth) die Mindestabstände einhalten. Siehe Planungsrichtlinie Mobile Access.

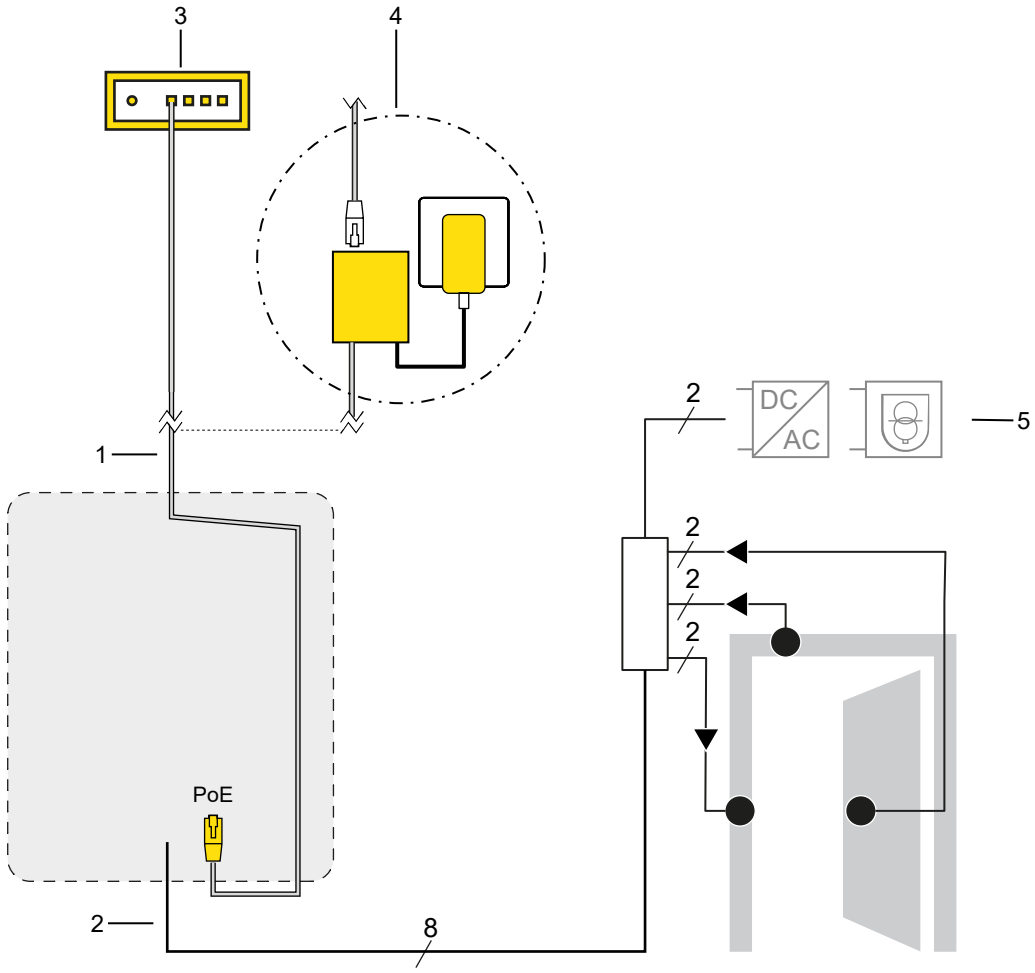
Überhitzung des Geräts vermeiden

- Gerät im ausreichenden Abstand zu Wärmequellen installieren.
- Gerät nicht an Orten mit direkter Sonneneinstrahlung installieren.

WLAN/Mobilfunk

- Vor der Installation prüfen, ob ausreichender Empfang gewährleistet ist.

5.1.2 Benötigte Leitungen und Stromversorgung



Leitungen

1 LAN
- mindestens CAT.5e, S/UTP
- mit RJ45-Stecker konfektioniert

2 Leitung zu Türkomponenten
- Leiterquerschnitt: 0,14 bis 0,5 mm² / AWG 26 bis 20
- Empfehlung: J-Y(ST)Y 4X2X0,8

Stromversorgung Gerät

3 PoE-Switch

oder

4 PoE-Injektor

Stromversorgung Türkomponenten

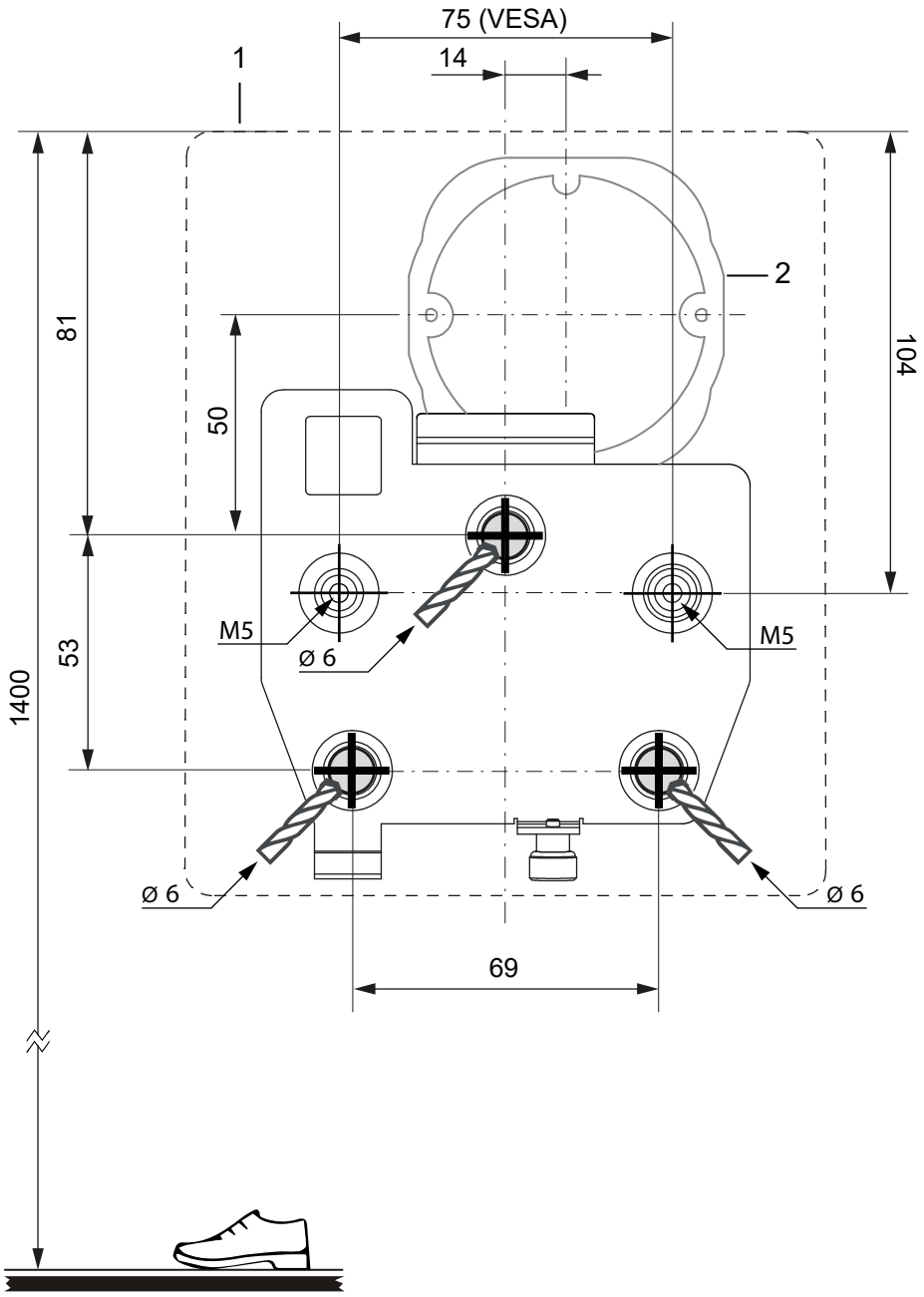
5 Netzteil

Netzteile müssen IEC/EN/UL/CSA 62368-1 konform sein.

5.2 Montageplatte an Wand schrauben

Gerät in geeignete Bedienungshöhe für alle Nutzende installieren.
Empfehlung: 140 cm von fertigem Fußboden bis zur Oberkante des Geräts.

Alternativ kann die Montageplatte mithilfe der M5-Gewinde auf eine Monitorhalterung (VESA MIS-D, 75x75 mm) geschraubt werden.



Alle Maße in mm.

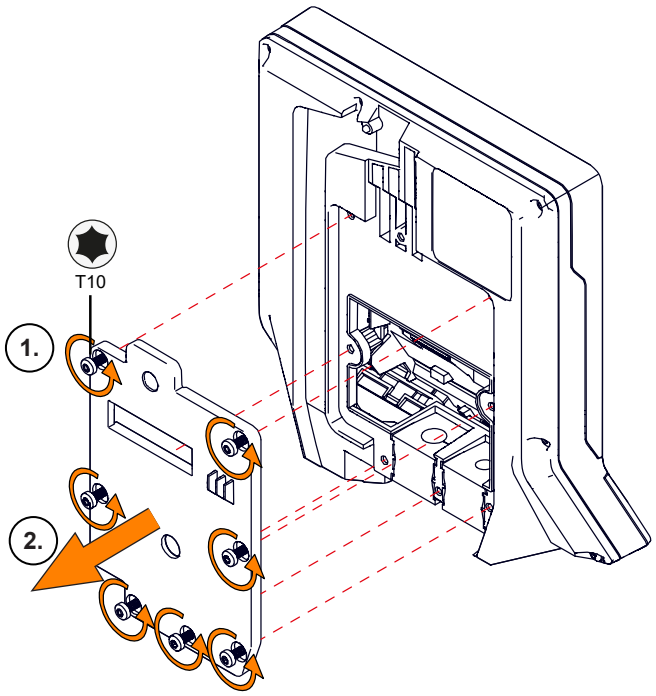
1 Gerätekontur

2 optional: UP-Gerätedose für Leitungen

1. 3 Bohrlöcher auf der Wand anzeichnen.
2. 3 Löcher in die Wand bohren.
3. 3 Dübel in die Löcher stecken.
4. Montageplatte positionieren und mit 3 Schrauben festschrauben.

5.3 Kabelabdeckung entfernen

Die Anschlüsse sind erst zugänglich, wenn die Kabelabdeckung entfernt ist.



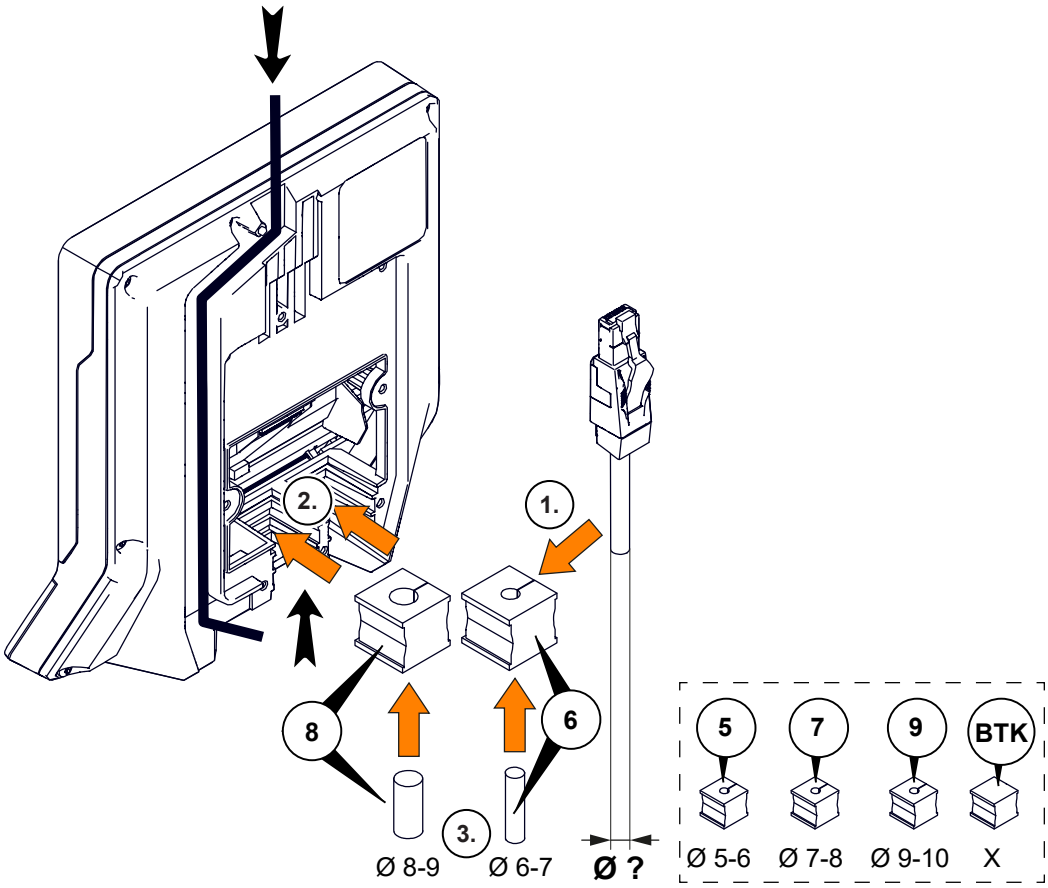
1. 7 Schrauben lösen.
2. Die Kabelabdeckung entfernen.

⇨ Die Anschlüsse sind zugänglich.

5.4 Leitungen ins Gerät einführen

Die Leitungen werden von unten in das Gerät eingeführt.

- Von oben kommende Leitungen durch den Kabelkanal nach unten führen.
- 2 Leitungen können eingeführt werden.



ACHTUNG

Werden falsche Teile verwendet, wird die Schutzart IP65 nicht eingehalten.

Um Schäden am Gerät zu vermeiden:

- Kabeltülle verwenden, die zum Leitungsdurchmesser passt.
  - ⇨ Ø 6-7 mm = Kabeltülle 6.
  - ⇨ Ø 8-9 mm = Kabeltülle 8.
  - ⇨ Ø 5-10 mm = Dichtungs-Set IP65 [▶ 14]
- Unbenutzte Kabeltülle mit passenden Kabeltüllenstopfen verschliessen.

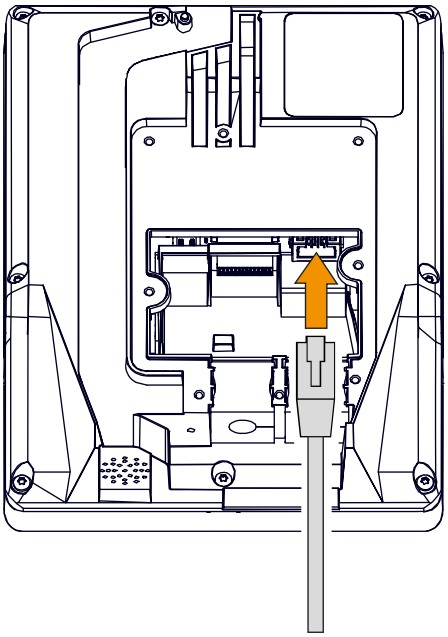
---

1. Leitung durch Kabeltülle führen.
2. Kabeltülle in die Führung schieben.
3. Optional (IP65): Unbenutzte Kabeltülle mit Kabeltüllenstopfen verschliessen.

5.5 Anschlüsse

5.5.1 Netzwerkkabel anschliessen

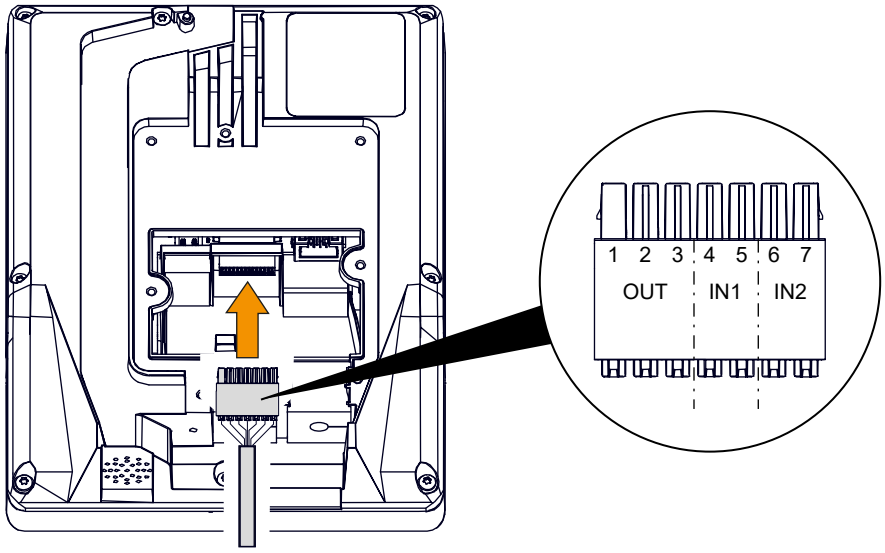
Die Kabelabdeckung vorher entfernen. Siehe Kabelabdeckung entfernen [▶ 23]



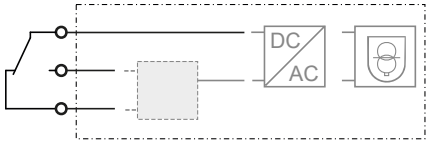
Das Netzwerkkabel in die RJ45-Buchse stecken.

5.5.2 Türkomponenten anschliessen

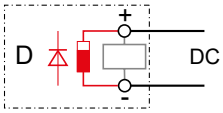
Die Kabelabdeckung vorher entfernen. Siehe Kabelabdeckung entfernen [▶ 23]

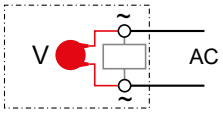


Ausgang (OUT)

Klemme	Belegung	Verdrahtung
1	C	
2	NO	
3	NC	

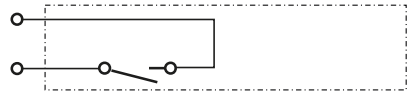
- Kontaktbelastbarkeit: 30 V AC/DC; max. 2 A
- Netzteile müssen IEC/EN/UL/CSA 62368-1 konform sein.
- Ist eine induktive Türkomponente (Türöffner, ...) nicht entstört, die Türkomponente durch einer der folgenden Maßnahmen entstören:





  - Gleichspannung (DC): Diode [D] parallel in Sperrrichtung anschliessen.
  - Wechselspannung (AC): Varistor [V] parallel anschliessen.

Eingänge (IN1-IN2)

Klemme	Belegung	Verdrahtung
4/6	GND	
5/7	IN1/IN2	

- Eingang ist aktiv, wenn Kontakt IN zu GND geschlossen ist.

5.5.3 USB-Komponente anschliessen

Werkseitig ist Verwendung von USB-Tastaturen deaktiviert.

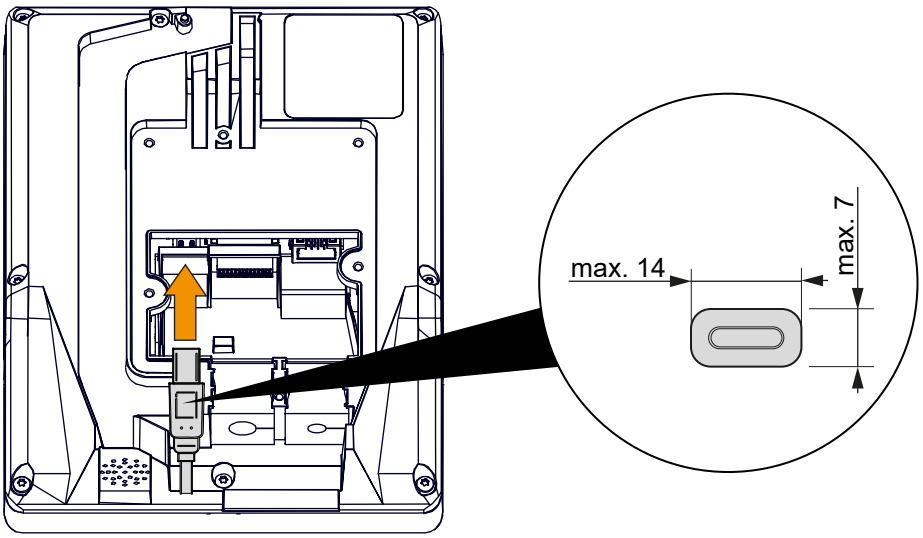
ACHTUNG

Verwendung nicht freigebener Barcodescanner

Werden Barcodescanner nicht über dormakaba bezogen, ist die Funktion nicht gewährleistet.

- Nur von dormaka freigegebenen Barcodescanner verwenden.
- Der Barcodescanner muss einen virtuellen COM-Port unterstützen.

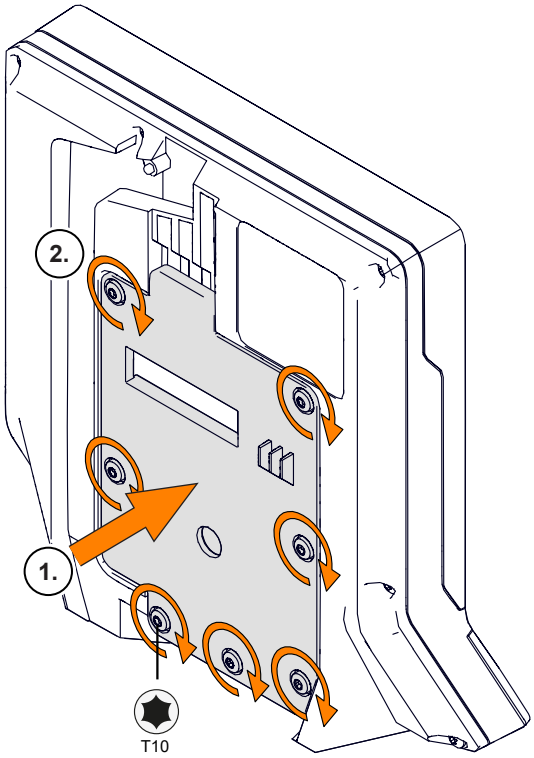
Die Kabelabdeckung vorher entfernen. Siehe Kabelabdeckung entfernen [▸ 23]



Das USB-Kabel in die USB-Buchse stecken.

5.6 Kabelabdeckung schliessen

Mit der original Kabelabdeckung ist die Schutzart IP20.
Zu Schutzart IP65, siehe Kabelabdeckung IP65 schliessen [▶ 29].



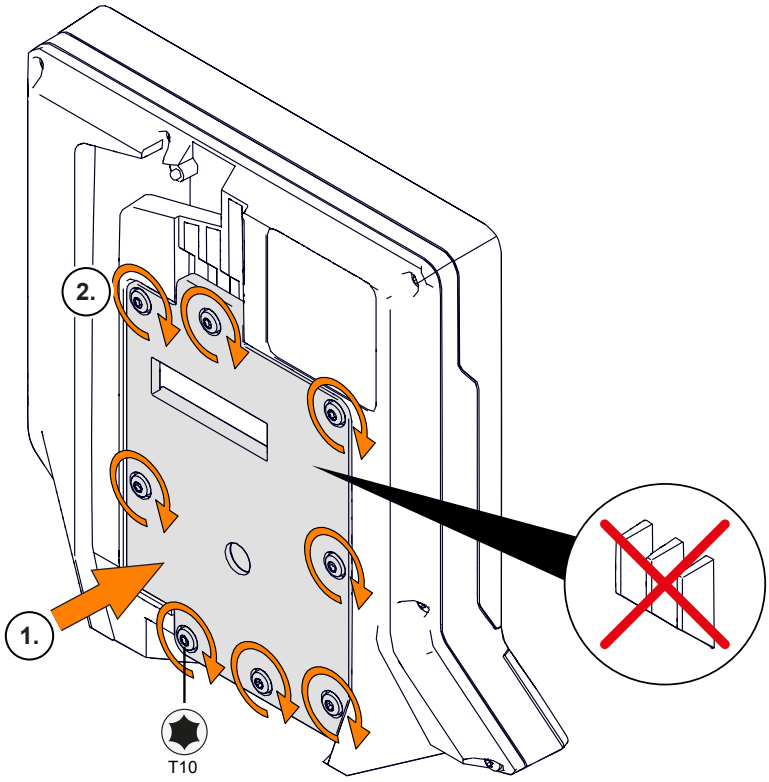
✓ Die Leitungen sind angeschlossen.

✓ Die Kabeltüllen sind eingesteckt.

1. Kabelabdeckung positionieren.
2. **Achtung!**
   Werden die Schrauben zu fest oder ungleichmäßig festgedreht, verbiegt sich die Kabelabdeckung.
   7 Schrauben festdrehen.

5.7 Kabelabdeckung IP65 schliessen

Die Kabelabdeckung aus dem Dichtungs-Set IP65 [▶ 14] verwenden.

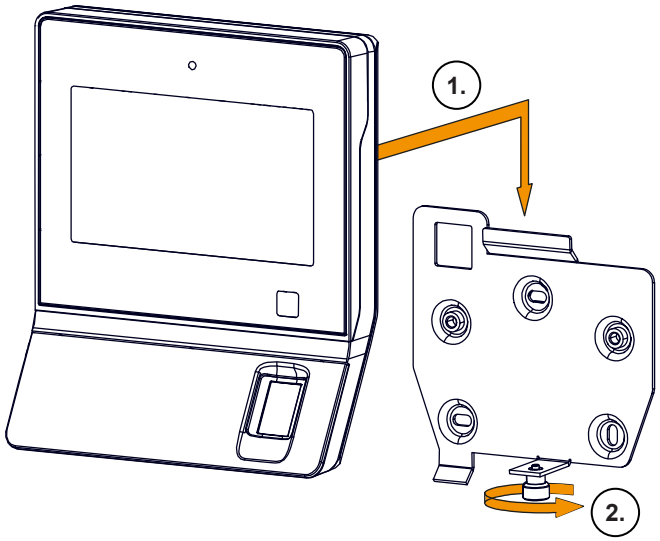


✓ Die Leitungen sind angeschlossen.

✓ Die Kabeltüllen sind eingesteckt.

1. Kabelabdeckung IP65 positionieren.
2. **Achtung!**
   Durch lose Schrauben wird die Schutzart IP65 nicht eingehalten. Um Schäden am Gerät zu vermeiden:
   8 Schrauben festdrehen.

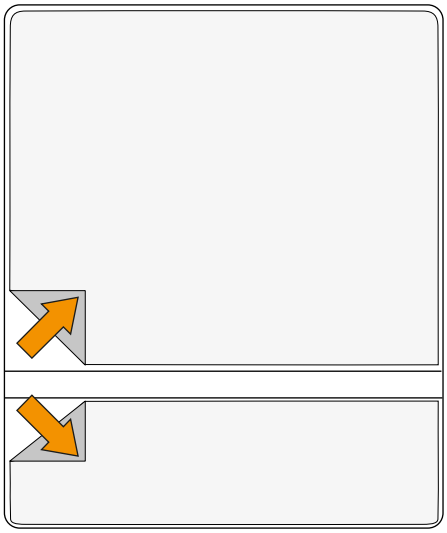
5.8 Terminal auf Montageplatte montieren



✓ Kabelabdeckung ist geschlossen.

1. Terminal an Montageplatte einhängen.
2. Terminal mit Schraube sichern.

5.9 Schutzfolien entfernen



Vor der Inbetriebnahme die 2 Schutzfolien entfernen.

6 Inbetriebnahme

6.1 LAN/WLAN Voraussetzungen

Server

- Ein **DHCP-Server** ist Voraussetzung für:
  - Automatische Zuweisung der IP-Adresse (Werkseinstellung)
  - Automatische Registrierung über B-COMM
- In der Windows Diensteverwaltung muss der Dienst SSDP aktiv sein.

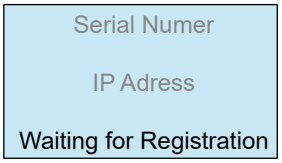
Firewall

In der Firewall müssen folgende Freigaben erteilt sein.

Protokoll/IP	Port		Verwendung
	dezimal	hexadezimal	
UDP	standard: 30464 Bereich: 30464 - 30703	7700 7700 - 77EF	Kommunikation mit Systemsoftware
UDP	1900	76C	• Automatische Registrierung über B-COMM • MATRIX Device Scanner
UDP/SSDP	30976	7900	Automatische Registrierung über B-COMM
UDP	standard: 30720 Bereich: 30720 - 30959	7800 7800 - 78EF	FTCS-Server
SSH/SFTP	22	16	SSH-Server
TCP	8443	20FB	Web-Server

6.2 Start der Inbetriebnahme

Sobald das Terminal an das LAN angeschlossen ist und über PoE mit Strom versorgt wird, befindet sich das Terminal auf Registrierung-Modus. Im Registrierung-Modus kann das Terminal automatisch über B-COMM registriert werden oder mit einer anderen Systemsoftware in Betrieb genommen werden.

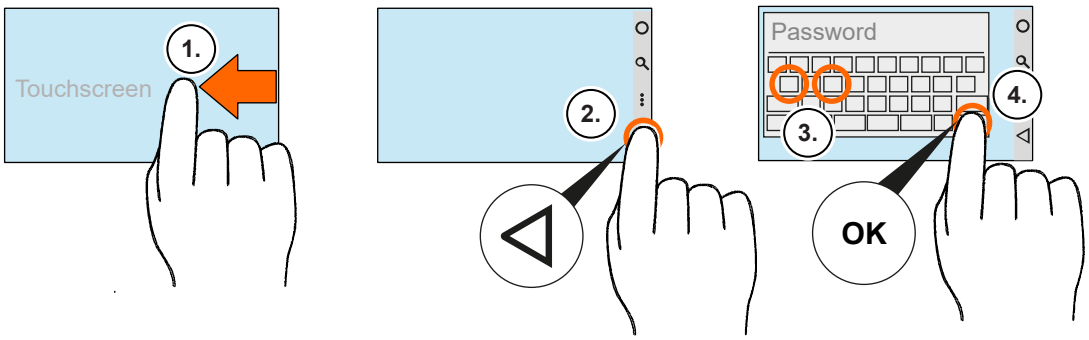


- Die Seriennummer des Terminals wird angezeigt.
- Die aktuelle IP-Adresse des Terminals wird angezeigt. Die Default-IP-Adresse ist: 123.0.0.2

Die Registrierung in folgenden Fällen abbrechen.

- Kein DHCP-Server im Netzwerk verfügbar.
- Feste IP-Adresse soll verwendet werden.
- IT-Sicherheitsregeln fordern Authentifizierung/Zertifikate für das Netzwerk.
- WLAN/Mobilfunk soll verwendet werden.

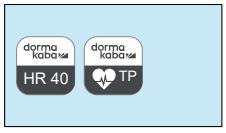
Registrierung abbrechen



1. Nach links wischen.
   ⇨ Die Navigationsleiste wird angezeigt.
2. Auf ◁ tippen und halten, bis Eingabemaske angezeigt wird.
3. Passwort eingeben.
   Hinweis: Beim 1. Aufruf muss das Passwort festgelegt werden.
4. Auf **OK** tippen.

⇨ Die automatische Registrierung ist abgebrochen.

⇨ Die Bedienoberfläche der BaseApp wird angezeigt.



⇨ Der Registrierung-Modus ist beendet.

⇨ Die Inbetriebnahme muss manuell durchgeführt werden.

6.3 Übersicht manuelle Inbetriebnahme

Die Tabelle gibt eine Übersicht welche Einstellungen bei der Inbetriebnahme vorgenommen werden müssen und welche Möglichkeiten es dafür gibt.

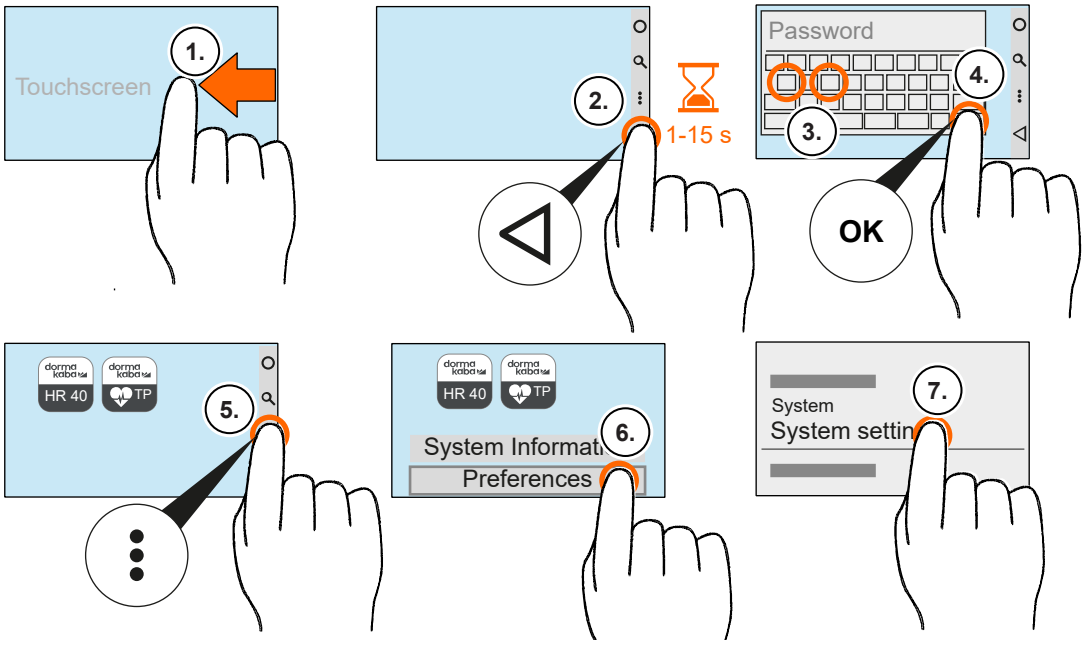
	Manuelle Inbetriebnahme	**lokal**			**Fernzugriff**		
		Android-Systemeinstellungen	Testprogramm	Service Interface - lokal	Service Interface - Fernzugriff	SFTP-Client	Systemsoftware
1.	Netzwerkeinstellungen ändern. • IP-Protokol: IPv4 oder IPv6 • Feste IP-Adresse	●	–	○	○	○	–
	Falls WLAN benutzt werden soll: • WLAN-Verbindung herstellen.	●	–	–	–	–	–
2.	Wenn es lokale IT-Sicherheitsregeln fordern: • Zertifikat einrichten • Authentifizierungsverfahren einrichten	○	–	–	●	○	–
3.	Service-Interface-Passwort ändern	–	–	●	●	○	○
4.	Bei folgendenden Leseverfahren den RFID-Leser intialisieren: • LEGIC mit AoC/DoC • LEGIC mit CardLink • MIFARE Baltech	–	–	–	–	–	–
	• MIFARE ARIOS	–	–	–	–	–	●

Legende

● empfohlen ○ alternativ – nicht möglich

6.4 Android Systemeinstellungen

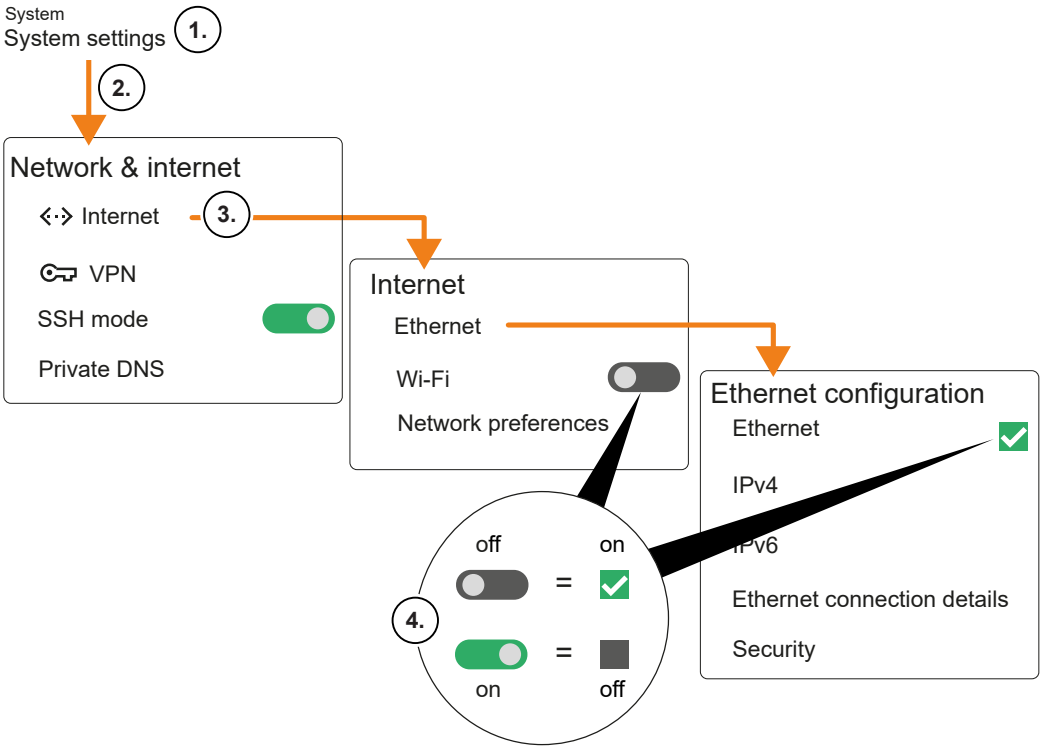
6.4.1 Android Systemeinstellungen aufrufen



1. Nach links wischen.
   ⇨ Navigationsleiste wird angezeigt.
2. Auf ◁ tippen und halten bis Eingabemaske erscheint.
   Hinweis: Die Dauer ist von 1 bis 15 Sekunden einstellbar. Default: 4 Sekunden
3. **Achtung!**
   Nach 3 ungültigen Passwort-Eingaben wird der Dialog gesperrt.
   Passwort eingeben. (Werkseitig: admin)
4. Auf **OK** tippen.
   ⇨ HR-Client ist beendet. Die BaseApp-Oberfläche wird angezeigt.
5. Auf ⋮ tippen.
6. Auf **Pereferences** (Einstellungen) tippen.
   ⇨ Andriod-Einstellungen wird geöffnet.
7. Auf **System setting** tippen.

6.4.2 Netzwerkeinstellungen ändern

✓ Android Systemeinstellungen aufrufen [▶ 34]

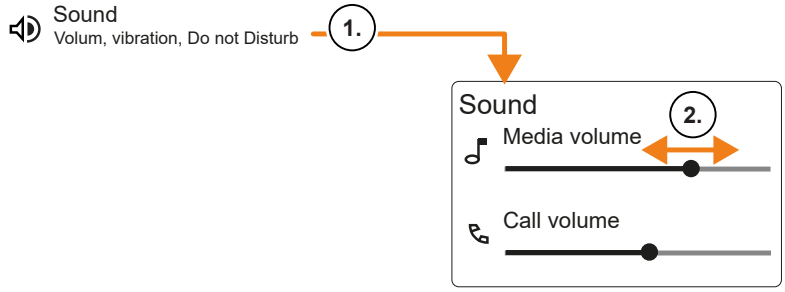


1. **System settings** auswählen.
2. **Network & internet** auswählen.
3. **Internet** auswählen.
4. **Ethernet** oder **Wi-Fi** (WLAN) einschalten.
   Hinweis:
   Durch Ein-/Ausschalten eines Netzwerktyps wird jeweils der andere Netzwerktyp ein- oder ausgeschaltet.

Ethernet (LAN)	Wi-Fi (WLAN)
1 **IPv4** oder **IPv6** auswählen. 2 **Connection type** auswählen. – Disable – DHCP – Static IP → IP-Adresse eingeben. → Gateway eingeben. → Netmask eingeben. → optional DNS1/DNS2 eingeben. 3 Mit **Done** bestätigen.	1 **Wi-Fi** auf **on** stellen. ⇒ Verfügbare **Wi-Fi-Netzwerke** werden angezeigt. 2 **Wi-Fi-Netzwerk** auswählen. 3 Abhängig vom Netzwerk: Die erforderlichen Eingaben eingeben. 4 Mit **Done** bestätigen.

6.4.3 Lautstärke ändern

✓ Android Systemeinstellungen aufrufen [▶ 34]



1. **Sound** auswählen.
2. Mit Schieberegler **Media volume** die Lautstärke einstellen.

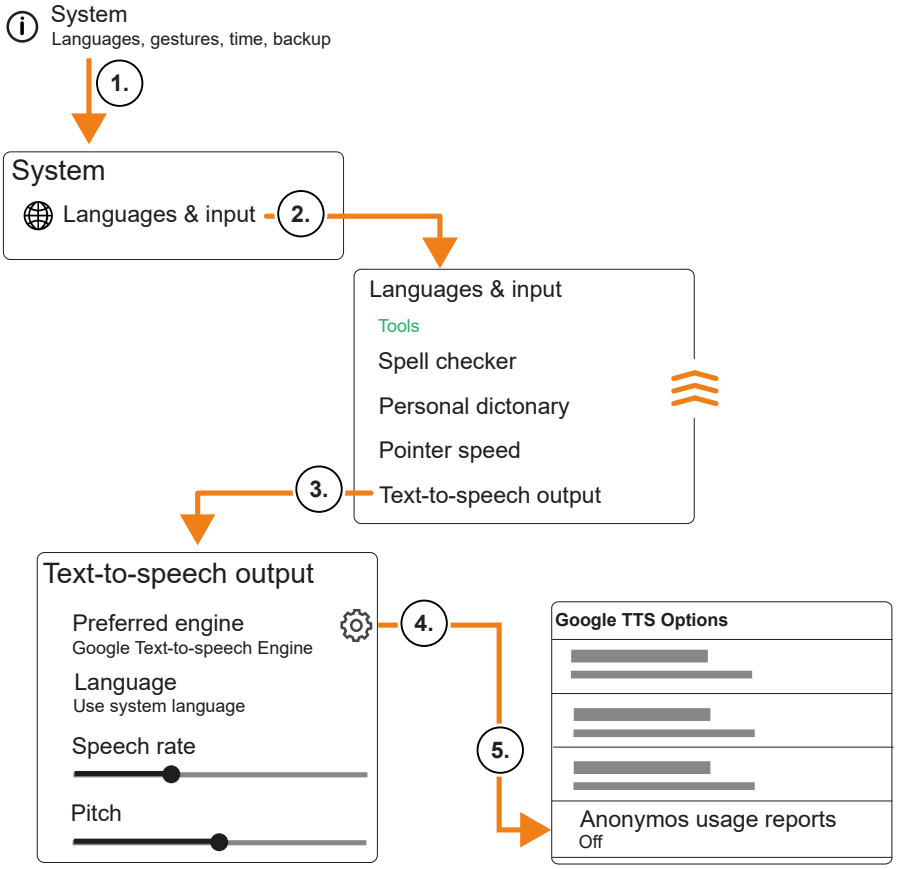
6.4.4 Sprachausgabe (Text to speech) aktivieren

Mit dieser Funktion werden Funktionstastentexte, Dialogtexte und Buchungsantworten dem Benutzer vorgelesen.

Voraussetzungen, um diese Funktion nutzen zu können:

- Die Funktion muss in der Gerätesoftware aktiviert sein. Siehe Referenzhandbuch B-Client HR40.
- Zum Herunterladen der Sprachdateien benötigt das Terminal einmalig eine Verbindung zum Internet.

✓ Android Systemeinstellungen aufrufen [▸ 34]

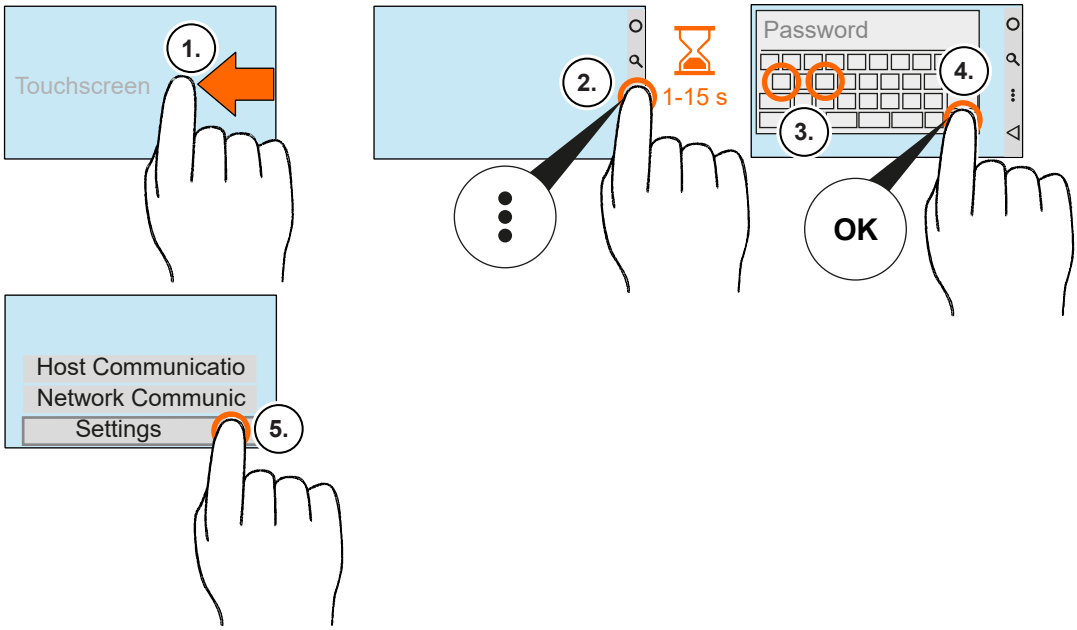


1. **System** auswählen.
2. **Languages & input** auswählen.
3. **Text-to-speech** auswählen.
4. **Google Text-to-speech Engine** aktivieren und Warnmeldung akzeptieren.
5. **Achtung!**
   Datenschutz: Die Erfassung von Benutzerdaten deaktivieren.

   Anonymos usage reports auf **Off** stellen.

6.5 Einstellungen mit Service Interface

6.5.1 Service Interface am Terminal aufrufen



1. Nach links wischen.
   ⇨ Navigationsleiste wird angezeigt.
2. Auf ⋮ tippen und halten bis Eingabemaske erscheint.
   Hinweis: Die Dauer ist von 1 bis 15 Sekunden einstellbar. Default: 4 Sekunden
3. Passwort eingeben. (Werkseitig: admin)
4. Auf **OK** tippen.
5. Auf **Settings** (Einstellungen) tippen.

⇨ Das Service Interface wird angezeigt.

Das Service Interface wird nach 3 Minuten automatisch geschlossen, wenn keine Eingabe erfolgt.

6.5.2 Service Interface am Rechner aufrufen

✓ Die IP-Adresse des Terminals ist bekannt.

✓ Der Web-Server des Terminals ist eingeschaltet.

1. Browser öffnen.
2. In die Adresszeile die IP-Adresse des Terminals eingeben. https://##.##.##.##:8443

   Sollte der Browser vor einem unbekannten Zertifikat warnen, bestätigen, dass die Seite vertrauenswürdig ist.

   ⇨ Das Anmeldefenster öffnet sich.
3. Passwort eingeben. (Werkseitig: admin)
4. Auf **Anmelden** klicken.

⇨ Das Service Interface wird angezeigt.

6.5.3 Service-Interface-Passwort ändern

ACHTUNG

Das werkseitige Passwort ist allgemein bekannt.

Um unbefugte Zugriffe zu vermeiden:

- Das werkseitige Passwort ändern und ein sicheres Passwort verwenden.

Wird das Terminal auf die Werkseinstellungen zurück gesetzt, wird auch das Passwort auf das werkseitige Passwort zurück gesetzt.

✓ Service Interface am Rechner aufrufen [▸ 38]
Service Interface am Terminal aufrufen [▸ 38]

1. Im Hauptmenü unter Settings **User management** auswählen.
   ⇨ Dialog **Change user passwords** wird angezeigt.
2. Altes Passwort eingeben.
3. Neues Passwort eingeben.
4. Neues Passwort bestätigen.
5. Auf **Submit** tippen.

⇨ Das Service-Interface-Passwort ist geändert.

6.5.4 Zertifikat mit Service Interface hochladen und einrichten

Dieser Vorgang ist nur über den Fernzugriff möglich.

✓ Das Zertifikat ist lokal auf dem Rechner gespeichert.

✓ Service Interface am Rechner aufrufen [▶ 38]

1. Im Hauptmenü unter Settings **Network** auswählen.
   ⇨ Dialogbereich mit 6 Tabs wird angezeigt. Nicht unterstützte Funktionen sind grau dargestellt.
2. Zu Tab **Certificate management** wechseln.
3. **IEEE802.1x certificate** auswählen.
   (standard: root certificate)
4. **Aliasname** und falls erforderlich **Password** eingeben.
5. Zertifikat hochladen.
   ⇨ Damit die Zertifikate angezeigt werden, muss im Browser die Seite neu geladen werden.
6. Einstellungen ändern und auf **Submit** tippen.
7. Im Hauptmenü zu **Administration** wechseln und auf **Reboot** tippen.

⇨ Das Zertifikat ist nach dem Neustart aktiv.

6.5.5 Authentifizierungverfahren mit Service Interface einrichten

Dieser Vorgang ist nur über den Fernzugriff möglich.

✓ Service Interface am Rechner aufrufen [▶ 38]

✓ Falls für das Authentifizierungverfahren ein Zerfifikat benötigt wird, Zertifikat mit Service Interface hochladen und einrichten [▶ 40]

1. Im Hauptmenü unter Settings **Network** auswählen.
   ⇨ Dialogbereich mit 6 Tabs wird angezeigt. Nicht unterstützte Funktionen sind grau dargestellt.
2. Zu Tab **Network security** wechseln.
3. Ein Authentifizierungverfahren auswählen und geforderte Eingaben eingeben.
   (standard: None)
4. Auf **Submit** tippen.
5. Im Hauptmenü zu **Administration** wechseln und auf **Reboot** tippen.

⇨ Das Authentifizierungverfahren ist nach dem Neustart aktiv.

6.6 Automatische Registrierung über B-COMM

Die Inbetriebnahme des Terminals erfolgt in Verbindung mit der Kommunikationssoftware B-COMM weitgehend automatisiert.

Das Gerät ist werksseitig für die automatische Registrierung über B-COMM voreingestellt.

Bei Kommunikation über WLAN muss die Verbindung zuvor eingerichtet und aktiviert werden. Dies erfolgt über die System-Einstellungen.

Systemvoraussetzungen

- Kommunikationssoftware B-COMM ab Version 5.3.1.2
- IPv4-basiertes Netzwerk mit einem funktionierenden DHCP-Server

Ablauf der Inbetriebnahme

1. Stromversorgung für das Gerät herstellen.
   - ⇨ Nach dem Systemstart meldet sich das Gerät zyklisch bei den im Netzwerk aktiven B-COMMs.
   - ⇨ In diesem Zustand wird, bis zur vollständigen Inbetriebnahme durch ein B-COMM, die Meldung "**Waiting for registration**" im Display angezeigt.
   - ⇨ Wird das Gerät von B-COMM erfasst, dann werden relevante Daten, die das Gerät identifizieren, abgefragt.
   - ⇨ Ist das Gerät nicht bekannt wird es in B-COMM unter dem Mandanten B-COMM Terminal Discovery unter dem Kanal BCTDS (Terminal Discovery Stream) eingetragen.
2. Gerät in B-COMM in den gewünschten Kommunikationskanal übernehmen.
3. Gerät mit den entsprechenden Kommunikations-Parametern versehen.
   - ⇨ Nachdem das Gerät in B-COMM fest zugeordnet wurde, aktualisiert B-COMM zunächst die Einstellungen des Gerätes und sichert diese zusammen mit der Lizenzdatei "sop.ini".
   - ⇨ Das Gerät teilt den im Netzwerk aktiven B-COMMs nun mit, dass die Registrierung erfolgt ist, wonach das Gerät von anderen B-COMMs wieder aus Kanal BCTDS entfernt wird.
4. Spezifische Parameter und Stammsätze auf das Gerät laden.

⇨ Die Gerätesoftware wird automatisch neu gestartet. Das Gerät ist danach betriebsbereit.

6.7 Leser-Initialisierung

Einige RFID-Leser müssen bei der Erstinbetriebnahme initialisiert werden.

6.7.1 LEGIC

Bei LEGIC-Lesern ist in bestimmten Fällen eine Leser-Taufe erforderlich:

- Wenn ein lesegeschütztes Segment verwendet werden soll.
- Wenn ein schreibgeschütztes Segment beschrieben werden soll, z. B. bei CardLink-Anwendung.

Taufe des Lesers

✓ Zur Taufe des Lesers ist eine SAM 63 Karte (Sicherheitskarte C2) mit dem entsprechenden Segment-Bereich erforderlich.

1. SAM 63 Karte vorhalten, wenn das Gerät im Normalbetrieb eine RFID-Eingabe erwartet.
   ⇨ Der Start des Vorganges wird durch ein akustisches Signal bestätigt.
   ⇨ Drei aufeinander folgende akustische Signale werden ausgegeben, wenn der Vorgang nicht ausgeführt werden kann, zum Beispiel wenn der Leser bereits getauft ist.
2. Die SAM 63 Karte muss sich etwa 15-20 Sekunden ununterbrochen im Lesefeld befinden.
   ⇨ Nach erfolgreicher Taufe werden 3 kurze akustische Signale ausgegeben.
   ⇨ Acht aufeinander folgende akustisches Signale werden ausgegeben, wenn ein Fehler aufgetreten ist.
3. SAM 63 Karte aus dem Feld entfernen.

Enttaufe des Lesers

✓ Die Enttaufe des Lesers erfolgt mit einer SAM 64 Karte.

1. SAM 64 Karte vorhalten, wenn das Gerät im Normalbetrieb eine RFID-Eingabe erwartet.
   ⇨ Der Start des Vorganges wird durch ein akustisches Signal bestätigt.
   ⇨ Drei aufeinander folgende akustische Signale werden ausgegeben, wenn der Vorgang nicht ausgeführt werden kann, zum Beispiel wenn der Leser bereits enttauft ist.
2. Die SAM 64 Karte muss sich etwa 15-20 Sekunden ununterbrochen im Lesefeld befinden.
   ⇨ Nach erfolgreicher Enttaufe werden 3 kurze akustische Signale ausgegeben.
   ⇨ Acht aufeinander folgende akustisches Signale werden ausgegeben, wenn ein Fehler aufgetreten ist.
3. SAM 64 Karte aus dem Feld entfernen.

6.7.2 MIFARE (ARIOS)

In Systemen mit ARIOS-Sicherheitskonzept muss der Anlagenschlüssel (EN: Sitekey) an die einzelnen Leser verteilt werden.

Der Anlagenschlüssel kann auf zwei Arten verteilt werden.

- Anlagenschlüssel-Verteilung über B-COMM.
- Anlagenschlüssel-Verteilung über Programmiermaster A oder B.

Details sind dem Referenzhandbuch der Gerätesoftware zu entnehmen.

6.7.3 MIFARE (Baltech)

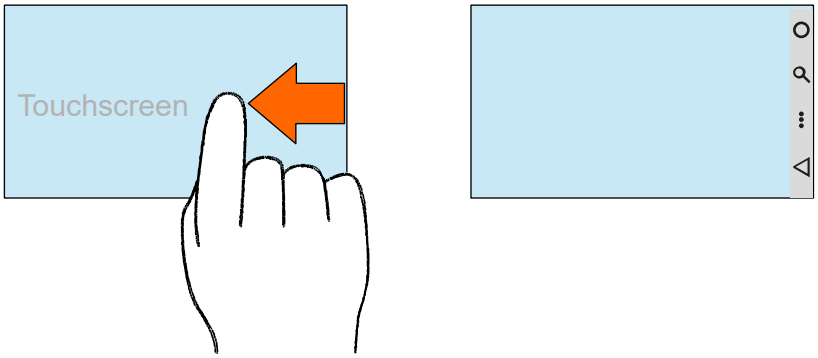
Der MIFARE-Leser muss mit einer MIFARE-Konfigurationskarte aktiviert werden:

1. Gerät ausschalten.
2. Gerät einschalten.
3. MIFARE-Konfigurationskarte ca. 10 Sekunden lang an den Leser halten.

7 Bedienung

7.1 Navigationstasten

Durch Wischen von der rechten Displaykante nach links, wird die Navigationsleiste angezeigt. Die Navigationsleiste enthält die Android-Navigationstasten.



Durch Berühren der einzelnen Symbole werden folgende Funktionen ausgeführt:

Home
Durch Berühren des Home-Symbols gelangt man in die Desktop-Ansicht (Startbildschirm) des Geräts. Da Android multitaskingfähig ist, laufen die aktiven Programme im Hintergrund weiter.

Suchen
Durch Berühren des Suchen-Symbols wird die Suchfunktion für das jeweils aktive Programm angezeigt.

Menü
Durch Berühren des Menü-Symbols wird ein Menü angezeigt, dessen Optionen sich auf das aktuelle Programm bzw. die aktuelle Bildschirmdarstellung beziehen.

Zurück
Durch Berühren des Zurück-Symbols kann jeweils zur letzten Displayansicht zurück gesprungen werden, also z. B. vom Untermenü ins Hauptmenü.

Wenn das System eine Eingabe erwartet, wird im Display eine virtuelle Tastatur angezeigt. In diesem Eingabe-Modus zeigt das Zurück-Symbol nach unten. Durch Berühren des Zurück-Symbols wir der Eingabe-Modus beendet und die virtuelle Tastatur ausgeblendet.

Die Home-Taste und die Suchen-Taste sind innerhalb der B-Client Gerätesoftware, des Testprogramms und der BaseApp ohne Funktion.

7.2 Symbole zur Bedienerführung

Die folgenden Standard-Symbole stehen der Gerätesoftware für die Bedienerführung zur Verfügung. Die Symbole sind Bestandteil der BaseApp.

Displayinhalte, Funktionen und Bedienabläufe sind abhängig von Einstellungen der Gerätesoftware.

7.2.1 Funktionstasten

Beispiele für Funktionstasten-Symbole. Weitere Varianten, sowie Symbole für weitere Funktionen stehen zur Verfügung.

Kommen

Gehen

Dienstgang

Abfrage

Sonderfunktion

7.2.2 Eingabeaufforderung

Die folgenden Symbole signalisieren dem Bediener, welche Eingabe aktuell erwartet wird.

Ausweis-Eingabe über den RFID-Leser erwartet.

Eingabe eines RFID-Ausweis mit Biometrie-Segment zur biometrischen Verifikation erwartet.

Eingabe des Fingers über den biometrischen Leser erwartet.

ID- oder PIN-Eingabe über die Tastatur erwartet.

Je nach System-Konfiguration sind alternativ mehrere Eingaben möglich. In diesem Fall werden mehrere Symbole für die möglichen Eingabearten gleichzeitig angezeigt.

7.2.3 Fehlerzustände

Die folgende Symbole signalisieren dem Bediener Fehlerzustände während einer Buchung.

Ungültige biometrische Verifikation

Kein Biometriesegment auf dem Ausweis erkannt oder Fehler beim Lesen des Finger-Template.

Ungültige biometrische Verifikation

Fingerabdruck ist nicht identisch mit dem Finger-Template auf dem Ausweis oder Finger-Template nicht vorhanden.

Ungültige biometrische Identifikation

In der Datenbank des CBM-Lesers befinden sich keine Finger-Templates (Datenbank leer).

Ungültige biometrische Identifikation

Finger ist in der Datenbank nicht vorhanden.

Lesefehler

Falsche Eingabe über die Tastatur

7.2.4 CardLink

Bei Verwendung der optionaler CardLink Funktion sind folgende Symbole relevant.

Ein CardLink Update ist verfügbar.

Während CardLink Validierung oder CardLink-Update ist ein Fehler aufgetreten.

7.2.5 Finger-Eingabe

Während der Fingerabdruck eingelesen wird, erfolgt eine ereignisgesteuerte Bedienerführung durch den biometrischen Leser.

Die folgenden Symbole werden im Display angezeigt, um dem Bediener Fehlerzustände anzuzeigen.

Finger muss weiter nach links.

Finger muss weiter nach rechts.

Finger muss weiter nach oben.

Finger muss weiter nach unten.

Finger fester aufdrücken.

Latenter Finger

Lesefenster des biometrischen Lesers reinigen.

In der Datenbank des CBM-Lesers befinden sich keine Finger- Templates (Datenbank leer).

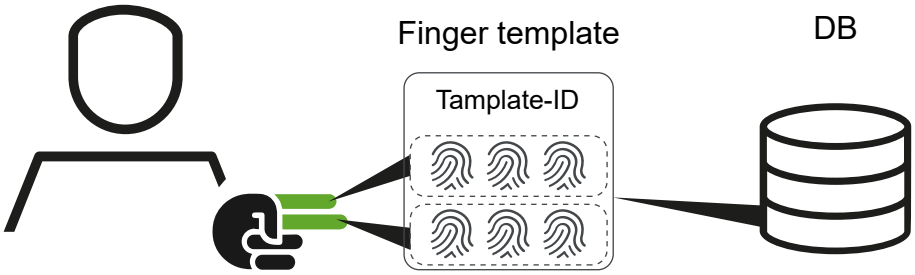
Dieser Zustand wird unmittelbar nach dem Aktivieren des Lesers angezeigt.

7.3 Local Enrollment: Fingerabdrücke mit Terminal verwalten

Voraussetzungen, um die Funktion **Local Enrollment** nutzen zu können:

- Das Terminal hat einen Fingerabdruckleser.
- Die Funktion ist lizenziert.
  Funktionsumfang der Lizenz anzeigen [▶ 60]

Die Fingerabdrücke werden mit dem internen Fingerabdruckleser erfasst und im internen Speicher des Fingerabdrucklesers gespeichert.



Pro Person werden 2 Finger mit je 3 Abdrücken erfasst. Zusammen mit der Tamplate-ID werden die Abdrücke als Finger-Tamplate in der Datenbank gespeichert.

Es gibt 2 Betriebsarten.

- **Mit Biometriesoftware**
  - Die Fingerabdrücke werden mit dem Finger Template Control Service (FTCS) synchronisiert und sind systemweit verfügbar.
  - Zum Erfassen von Fingerabdrücken (Enroll) wird eine FTCS-Verbindung über den BCFTC-Kanal benötigt.
- **Standalone**
  - Nur die lokal erfassten Fingerabdrücke sind verfügbar.

Es gibt 5 Unterfunktionen.

1 **ENROLL**
Enroll: Fingerabdrücke einer Person erfassen [▶ 50]

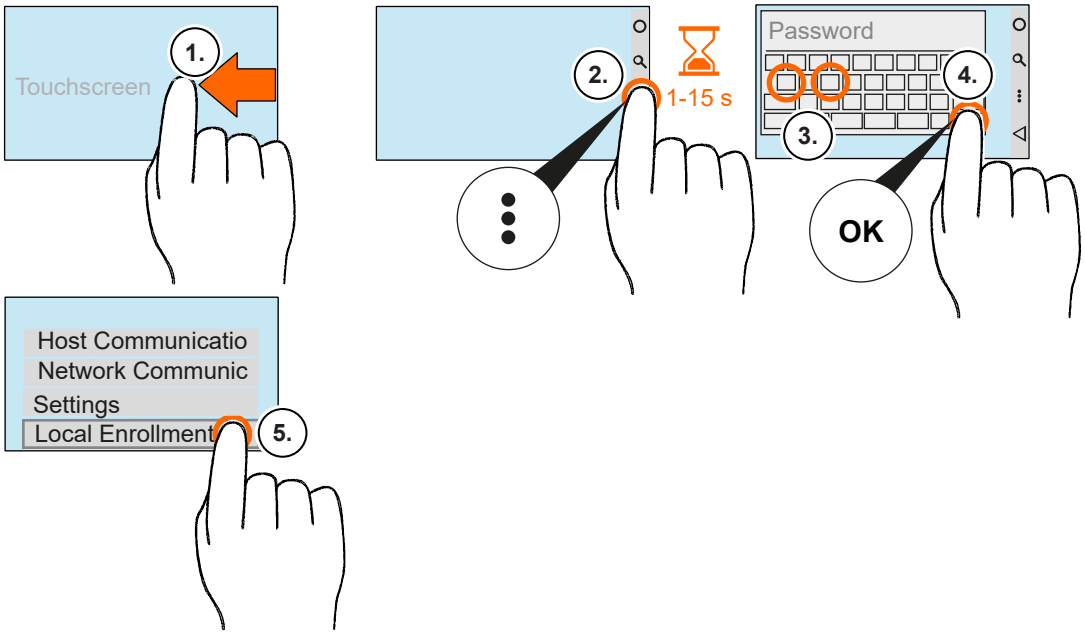
2 **UNENROLL**
Unenroll: Finger-Template löschen [▶ 51]

3 **IDENTIFY**
Zeigt die Tamplate-ID einer Person an, wenn die Fingerabdrücke bereits erfasst sind. Die Person muss einen gespeicherten Finger auf den Fingerabdruckleser legen.

4 **LIST**
Zeigt alle in der Datenbank gespeicherten Tamplate-IDs an. Die Funktion ist nur verfügbar, wenn weniger als 100 Template-IDs gespeichert sind.

5 **ERASE DB**
Löscht alle gespeicherten Finger-Template aus der Datenbank. Der Vorgang ist durch die Erase-PIN **439235** geschützt.

7.3.1 Local Enrollment aufrufen



1. Nach links wischen.

   ⇨ Navigationsleiste wird angezeigt.

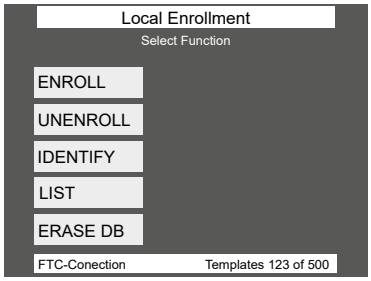
2. Auf ⋮ tippen und halten bis Eingabemaske erscheint.
   Hinweis: Die Dauer ist von 1 bis 15 Sekunden einstellbar. Default: 4 Sekunden

3. **Achtung!**
   Nach 3 ungültigen Passwort-Eingaben wird der Dialog gesperrt.
   Passwort eingeben. (Werkseitig: admin)

4. Auf **OK** tippen.

5. Auf **Local Enrollment** tippen.

⇨ Das Hauptfenster von **Local Enrollment** wird angezeigt.



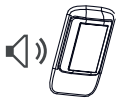
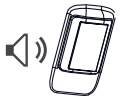
7.3.2 Enroll: Fingerabdrücke einer Person erfassen

✓ Local Enrollment aufrufen [▸ 49]

1. **Enroll** auswählen.
2. **Template-ID** eingeben.
   Hinweis
   Anhand der Template-ID wird die Person identifiziert. Die Länge der Template-ID ist durch den Parameter **PresetEnroll** vorgegeben.
3. Auf **OK** tippen.
   ⇨ Ein neues Fenster wird angezeigt.
4. 2 Finger der Person jeweils 3x erfassen.

   Je Erfassungsvorgang wird ein Qualitätswert angegeben.

   > 120 = sehr gut 60 - 120 = gut < 60 = schlecht

1. Finger auf den Fingerabdruckleser legen und nach dem Signal-Ton entfernen.			
1. Finger auf den Fingerabdruckleser legen und nach dem Signal-Ton entfernen.			
1. Finger auf den Fingerabdruckleser legen und nach dem Signal-Ton entfernen.			
2. Finger auf den Fingerabdruckleser legen und nach dem Signal-Ton entfernen.			
2. Finger auf den Fingerabdruckleser legen und nach dem Signal-Ton entfernen.			
2. Finger auf den Fingerabdruckleser legen und nach dem Signal-Ton entfernen.			
		Alle Finger erfolgreich erfasst.	

Ist die Qualität eines Fingers schlecht, den Vorgang wiederholen.

Ist die Qualität eines Fingers wiederholt schlecht, einen anderen Finger erfassen.

5. Das Template speichern.

⇨ Die Fingerabdrücke der Person sind erfasst.

7.3.3 Unenroll: Finger-Template löschen

✓ Local Enrollment aufrufen [▶ 49]

1. **Unenroll** auswählen.
2. **Finger-Template** auswählen via

   - **Numpad**

     Die Template-ID über die virtuelle Tastatur eingeben.
   - **Reader**

     Ein erfasster Finger von der Person auf den Fingerabdruckleser legen.
   - **List**

     Die Template-ID wird aus der Liste wählen.

8 Reinigung des Gehäuses

Zur Reinigung des Gehäuses ein weiches, nicht flusendes Tuch und ein mildes Fensterreinigungsmittel verwenden!

ACHTUNG

Schäden am Gehäuse durch ungeeignete Reinigungsmittel

Um das Gehäuse durch den Reinigungsvorgang nicht zu beschädigen, bitte Folgendes beachten:

- keinen Alkohol wie Ethanol oder Isopropanol verwenden
- keine scharfen Lösungsmittel verwenden
- kein Reinigungsmittel mit Pulverzusatz verwenden
- kratzende und scheuernde Bewegungen vermeiden

9 Wartung

9.1 Übersicht Wartung

Die Tabelle gibt eine Übersicht über mögliche Wartungsaufgaben und welche Möglichkeiten es dafür gibt.

Wartungsaufgabe	lokal			Fernzugriff				
	Android-Systemeinstellungen	Testprogramm	Service Interface - lokal	Service Interface - Fernzugriff	SFTP-Client	SFTP-Installer	SSH-Client	Systemsoftware
Gerätesoftware aktualisieren [▶ 54]	–	–	–	–	–	●	–	–
RFID-Leser: Installierte Firmware-Version anzeigen [▶ 55]	–	●	–	–	–	–	–	–
RFID-Leser: Firmware aktualisieren [▶ 55]	–	–	–	●	–	–	–	–
Web-Server ein- oder ausschalten [▶ 56]	●	–	–	–	○	–	–	○
SSH-Server ein- oder ausschalten [▶ 56]	●	–	–	–	○	–	–	○
Terminal-Passwort ändern	–	–	–	–	○	–	–	●
Terminal-Passwort-Sperre aufheben	–	–	–	–	○	–	–	●
Service-Interface-Passwort ändern [▶ 39]	–	–	●	●	○	–	–	–
USB-Tastatur mit SSH-Client aktivieren [▶ 57]	–	–	–	–	–	–	●	–
USB-Tastatur mit SSH-Client deaktivieren [▶ 58]	–	–	–	–	–	–	●	–
Funktionsumfang der Lizenz anzeigen [▶ 60]	–	–	●	●	–	–	–	–
Funktionsumfang mit neuer Lizenz erweitern [▶ 61]	–	–	–	–	–	●	–	–
Systeminformationen anzeigen [▶ 61]	○	–	●	●	–	–	–	–
Diagnosedaten für Support bereitstellen	–	–	–	●	–	–	–	–

Legende

- ● empfohlen
- ○ alternativ
- – nicht möglich

9.2 Gerätesoftware aktualisieren

Firmware, Gerätesoftware und weitere Software sind im **my.dormakaba Portal** verfügbar.
https://portal-dormakaba.onelogin.com

Die Gerätesoftware wird mit dem **SFTP-Installer** aktualisiert.

Gerätesoftware, Apps und SFTP-Installer werden als ZIP-Datei bereitgestellt. Sollte es eine neue Android-Version geben, ist diese ebenfalls enthalten.

Bei der Ausführung wird zwischen **Update** oder **Installation** unterschieden.

- **Update**

  Die Gerätesoftware wird auf eine neue Version aktualisiert. Aktuelle Einstellungen bleiben erhalten.

- **Installation**

  Die Gerätesoftware wird neu installiert. Aktuelle Einstellungen gehen verloren und das Terminal muss neu in Betrieb genommen werden. Eine fehlerhafte Installation kann damit repariert werden.

✓ SSH-Server des Terminals ist eingeschaltet.
SSH-Server ein- oder ausschalten [▸ 56]

✓ SFTP-Installer wurde heruntergeladen.

✓ Nur bei Installation: Gerätekonfiguration und Parametrierung sind gesichert.

✓ Falls es kundenspezifische Layout-Anpassungen gibt, die Datei **interface.ini** und entsprechende Bilder sind vom Terminal herunterladen und gesichert.

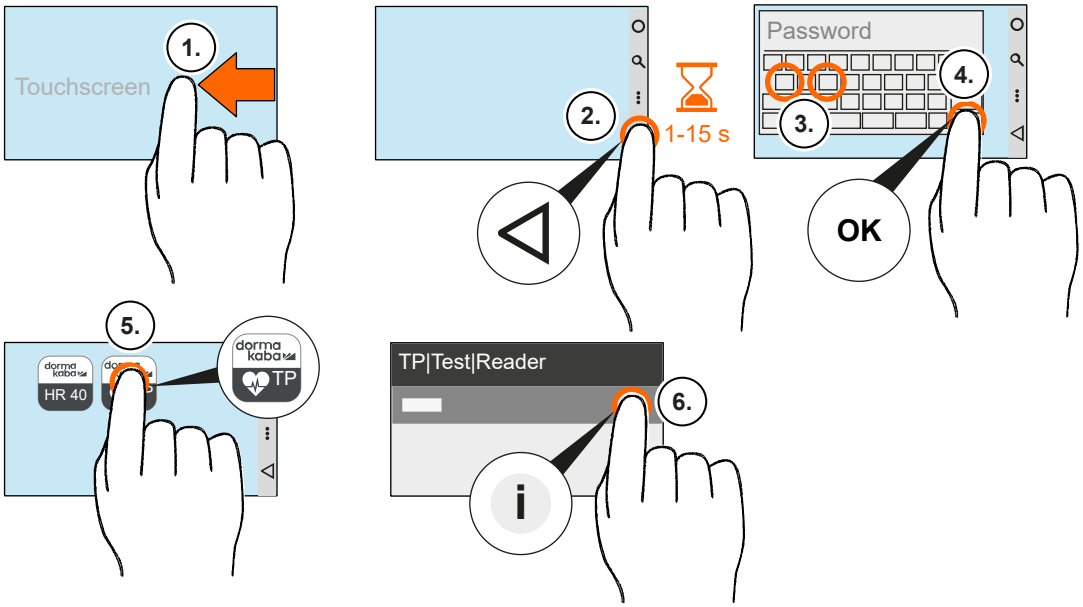
1. SFTP-Installer (ZIP-Datei) in ein Verzeichnis auf dem Rechner entpacken.
2. Falls SSH-Schlüsseldatei geändert wurde, die kundenspezifische SSH-Schlüsseldatei in das entpackte Verzeichnis kopieren.
3. Doppelklick auf **SFTP Installer.exe** ausführen.

   Wird eine Sicherheitswarnung angezeigt, auf Ausführen klicken.

   ⇨ SFTP Installer wird geöffnet.
4. Die Handlungsanweisungen der Bedienoberfläche befolgen.
5. Terminal neu starten.

⇨ Die Gerätesoftware ist aktualisiert.

9.3 RFID-Leser: Installierte Firmware-Version anzeigen



1. Nach links wischen.
   ⇨ Navigationsleiste wird angezeigt.
2. Auf ◁ tippen und halten bis Eingabemaske erscheint.
   Hinweis: Die Dauer ist von 1 bis 15 Sekunden einstellbar. Default: 4 Sekunden
3. **Achtung!**
   Nach 3 ungültigen Passwort-Eingaben wird der Dialog gesperrt.
   Passwort eingeben. (Werkseitig: admin)
4. Auf **OK** tippen.
5. Auf ⋮ tippen.
6. Auf **TP** (Testprogramm) tippen.
   ⇨ Testprogramm wird geöffnet.
7. Auf **Test/leser** tippen.
8. Auf **Info** tippen.

⇨ Die Installierte Firmware-Version wird angezeigt.

9.4 RFID-Leser: Firmware aktualisieren

Firmware, Gerätesoftware und weitere Software sind im **my.dormakaba Portal** verfügbar.
https://portal-dormakaba.onelogin.com

✓ Web-Server des Terminals ist eingeschaltet.
Web-Server ein- oder ausschalten [▸ 56]

✓ RFID-Leser-Firmware ist auf dem Rechner gespeichert.

✓ Service Interface ist am Rechner aufgerufen.
[siehe Service Interface am Rechner aufrufen [▸ 38]]

1. Im Hauptmenü unter FIRMWARE **Firmware update** auswählen.
   ⇨ Dialogbereich wird angezeigt.
2. Firmware-Datei auswählen.
3. Auf **Start update** klicken.

9.5 Web-Server ein- oder ausschalten

ACHTUNG

IT-Sicherheitsrisiko durch eingeschalteten Web-Server.

Über den Web-Server kann unberechtigt auf das Terminal zugegriffen werden.

- Web-Server nach Inbetriebnahme/Wartung ausschalten.

Das Service Interface steht nur zur Verfügung, wenn der Web-Server eingeschaltet ist.

✓ Android Systemeinstellungen aufrufen [▸ 34]

1. Zu **Service Interface** navigieren.
2. Web-Server ein- oder ausschalten.
   - ⇨ ☐ Web-Server aus
   - ⇨ ☑ Web-Server ein

9.6 SSH-Server ein- oder ausschalten

ACHTUNG

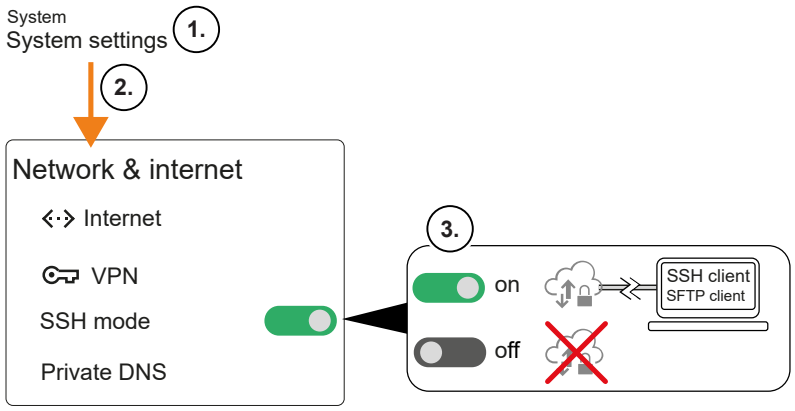
IT-Sicherheitsrisiko durch eingeschalteten SSH-Server.

Über den SSH-Server kann unberechtigt auf das Terminal zugegriffen werden.

- SSH-Server nach Inbetriebnahme/Wartung ausschalten.

Ein Zugriff mit einem SFTP-Client oder SSH-Client ist nur möglich, wenn der SSH-Server eingeschaltet ist.

✓ Android Systemeinstellungen aufrufen [▸ 34]



1. **System settings** auswählen.
2. **Network & internet** auswählen.
3. Schalter **SSH mode** ein- oder ausschalten.

9.7 SSH-Client mit Terminal verbinden

✓ **SSH-Client** (z.B. PuTTY) ist auf dem Rechner installiert.

✓ **SSH-Server** auf dem Terminal ist eingeschaltet.
SSH-Server ein- oder ausschalten [▸ 56]

✓ **SSH-Schlüsseldatei** ist vorhanden.
standard: kaba-private-ssh-key.ppk, falls SSH-Schlüsseldatei geändert wurde, die kundenspezifische SSH-Schlüsseldatei verwenden.

1. SSH-Client starten.
2. Verbindung einrichten.

Einstellung	Wert
Connection Type	SSH/Telnet
Serveradresse	<IPv4-Adresse des Terminals>
Port	22
Benutzername	root
Passwort	kaba
Connection → SSH → AUTH → Credentials → Private key file	<Pfad zur SSH-Schlüsseldatei>

3. Auf **Open** klicken.
   ⇨ Kommando-Fenster wird angezeigt.
4. Login as **root** eingeben.
5. **Passphrase** eingeben. (**kaba** oder kundenspezifische)

⇨ Terminal-Kommandos können ausgeführt werden.

9.8 USB-Tastatur mit SSH-Client aktivieren

Werkseitig ist Verwendung von USB-Tastaturen deaktiviert.

ACHTUNG

Ist die Verwendung von USB-Tastaturen aktiviert, kann über eine USB-Tastatur unberechtigt auf die Systemeinstellungen zugegriffen werden.

USB-Tastatur nur kurzzeitig für Servicearbeiten aktivieren.

✓ USB-Tastatur ist nicht in die USB-Buchse eingesteckt.

✓ SSH-Client mit Terminal verbinden [▸ 57]

1. Kommando `setprop kdb.input.device.disable 0` eingeben und mit **Eingabetaste** bestätigen.
2. (Einstellung prüfen.)
   Kommando `getprop kdb.input.device.disable` eingeben und mit **Eingabetaste** bestätigen.
   ⇨ 0 muss angezeigt werden.
3. USB-Tastatur in die USB-Buchse einstecken.

⇨ USB-Tastatur ist aktiviert.

9.9 USB-Tastatur mit SSH-Client deaktivieren

✓ USB-Tastatur ist in die USB-Buchse eingesteckt.

✓ SSH-Client ist mit Terminal verbunden.
SSH-Client mit Terminal verbinden [▶ 57]

1. Kommando `setprop kdb.input.device.disable 1` eingeben und mit **Eingabetaste** bestätigen.
2. (Einstellung prüfen.)
   Kommando `getprop kdb.input.device.disable` eingeben und mit **Eingabetaste** bestätigen.

   ⇨ 1 muss angezeigt werden.
3. USB-Tastatur aus der USB-Buchse ziehen.

⇨ USB-Tastatur ist deaktiviert.

9.10 Mit SFTP-Client auf Terminal-Dateien zugreifen

ACHTUNG

Löschen, Verschieben und Ändern von Dateien

Fehlerhafte Aktionen führen zu Fehlfunktionen oder Geräteausfall.

- Richtige Verzeichnisse/Dateien verwenden
- Vor dem Ändern einer Datei, eine Sicherheitskopie erstellen.
- Die vorgegebene Syntax bei Datei-Inhalten beachten.

✓ **SFTP-Client** (z.B. WinSCP) ist auf dem Rechner installiert.

✓ **SSH-Server** auf dem Terminal ist eingeschaltet.
SSH-Server ein- oder ausschalten [▸ 56]

✓ **SSH-Schlüsseldatei** ist vorhanden.
standard: kaba-private-ssh-key.ppk, falls SSH-Schlüsseldatei geändert wurde, die kundenspezifische SSH-Schlüsseldatei verwenden.

1. SFTP-Client starten.
2. Verbindung einrichten.

Einstellung	Wert
Übertragungsprotokoll	SFTP
Serveradresse	<IPv4-Adresse des Terminals>
Port	22
Benutzername	root
Passwort	kaba
SSH-Authentifizierung → Privater Schlüssel	<Pfad zur Datei>

3. Auf Anmelden klicken.
   ⇨ Fenster Passphrase wird angezeigt.
4. **Passphrase** eingeben. (**kaba** oder kundenspezifische)

⇨ Fenster mit Dateienverzeichnis Rechner/Terminal wird angezeigt.

9.11 Funktionsumfang der Lizenz anzeigen

Der Funktionsumfang des Terminals ist abhängig von Optionen. Optionen werden mit einem Lizenz-Schlüssel frei geschaltet.

✓ Service Interface am Terminal aufrufen [▸ 38]
Service Interface am Rechner aufrufen [▸ 38]

1. Im Hauptmenü unter System **Licence** auswählen.

⇨ Der Funktionsumfang der aktuellen Lizenz wird durch die Parameter angezeigt.

Eintrag	Bedeutung
`CardLinkEnabled=`	CardLink Funktion
`EncryptionEnabled=`	Datenverschlüsselung über UDP und HTTPS
`AccessControlEnabled=`	Türsteuerung
`LocalEnrollmentEnabled=`	Erfassen von Fingerabdrücken am Terminal.
`PartnerInterfaceEnabled=`	Unterstützung von Partner-Applikationen
`NativeAppEnabled=`	Start nativer Apps durch die Gerätesoftware (HR)
`Browserenabled=`	Browser-Aufruf durch die Gerätesoftware
`MobileAccessEnabled=`	Buchen mit Hilfe eines Smartphon in Verbindung mit einem MRD-Leser
`AdditionalInputStepsEnabled=`	Zusätzliche Eingabeschritte während eines Buchungsvorganges

Sonstige Parameter

Eintrag	Bedeutung
`ReplacementEnabled=true`	Durch dormakaba geliefertes Austauschgerät Dieses Gerät muss über das 1-Click-Replacement in Betrieb genommen werden.

Lizenz-bezogene Parameter

Eintrag	Bedeutung
`ExpiryDate=`	Gültigkeitsdatum
`Key=`	Lizenzschlüssel
`MAC=`	MAC-Adresse
`CreationDate=`	Erstellungsdatum

Test-Lizenz-bezogene Parameter

Eintrag	Bedeutung
`TmpLicKeyCnt=`	Zeigt an wie viel mal auf diesem Gerät noch eine Testlizenz erzeugt werden kann.
`TestLicenceEnabled=true`	Diese Lizenzdatei ist eine temporäre Testlizenz

9.12 Funktionsumfang mit neuer Lizenz erweitern

Der Funktionsumfang kann durch den Erwerb zusätzlicher Optionen erweitert werden. In diesem Fall muss die vorhandene Lizenzdatei durch die neu erworbene Lizenzdatei ersetzt werden.

ACHTUNG

Die Lizenzdatei ist ungültig, wenn der Inhalt geändert wird.

Eine ungültige Lizenzdatei verursacht Fehlfunktionen.

- Den Inhalt der Lizenzdatei nicht ändern.

ACHTUNG

Die Lizenzdatei ist ungültig, wenn eine falsche MAC-Adresse entalten ist.

Eine ungültige Lizenzdatei verursacht Fehlfunktionen.

- Sicherstellen, dass die MAC-Adresse übereinstimmt.

✓ Neue Lizenzdatei (sop-ini) ist vorhanden.

✓ Mit SFTP-Client auf Terminal-Dateien zugreifen [▸ 59]

1. Im SFTP-Client zu Lizenz-Verzeichnis des Terminals navigieren.
   /data/data/com.kaba.apps.hr/files/init
2. Die neue Lizenzdatei in das Verzeichnis kopieren.
3. Das Terminal neu starten.

⇨ Die Funktionen der neuen Lizenz können genutzt werden.

9.13 Systeminformationen anzeigen

✓ Service Interface am Rechner aufrufen [▸ 38]

1. Im Hauptmenü unter System **System information** auswählen.

⇨ Systeminformationen werden angezeigt.

10 Verpackung/Rücksendung

Nicht ordnungsgemäß verpackte Baugruppen und Geräte können durch Beschädigungen während des Transports Kosten verursachen.

Bitte folgende Hinweise beachten, wenn dormakaba Produkte versendet werden.

dormakaba haftet nicht für Schäden an Produkten, die auf eine unzureichende Verpackung zurückzuführen sind.

10.1 Komplettgeräte

Die Originalverpackung ist speziell an das Gerät angepasst. Sie bietet größtmöglichen Schutz vor Transportschäden.

Zur Rücksendung immer die Originalverpackung verwenden!

Sollte dies nicht möglich sein, so ist für eine Verpackung zu sorgen, welche eine Beschädigung des Gerätes ausschließt.

- Eine stabile, dickwandige Transportkiste oder einen Karton verwenden. Die Transportkiste sollte so groß sein, dass zwischen Gerät und Behälterwand 8-10 cm Platz bleibt.
- Gerät mit einer geeigneten Folie umhüllen oder in einen Beutel geben.
- Gerät rundherum großzügig polstern, z. B. mit Schaumpolstern oder Luftkissen. Ein Wandern des Gerätes innerhalb der Verpackung muss ausgeschlossen sein.
- Ausschließlich staubfreies und umweltverträgliches Füllmaterial verwenden.

10.2 Beschriftung

Komplette Rücksendungspapiere und eine korrekte Beschriftung ermöglichen uns eine schnelle Abwicklung. Bitte sicherstellen, dass jedem Packstück ein Lieferschein beigefügt ist. Der Lieferschein sollte folgende Informationen beinhalten:

- Anzahl der Geräte oder Komponenten pro Packstück.
- Artikelnummern, Seriennummern, Bezeichnungen, Bestellnummer.
- Adresse Ihres Unternehmens/Ansprechpartners.
- Grund der Rücksendung, z. B. Reparaturaustausch.
- Aussagekräftige Fehlerbeschreibung.

Bei Rücksendungen aus Ländern außerhalb der EU ist zusätzlich eine Zollrechnung mit reellem Zollwert und Zolltarifnummer erforderlich.

11 Entsorgung

Das Gerät ist mit dem nebenstehenden Symbol gekennzeichnet, das auf das Verbot der Entsorgung über den Hausmüll hinweist.

Die Bestandteile des Gerätes müssen getrennt der Wiederverwertung oder Entsorgung zugeführt werden. Altgeräte enthalten wertvolle recyclingfähige Materialien, die einer Verwertung zugeführt werden müssen. Giftige und gefährliche Bestandteile können bei unsachgemäßer Entsorgung die Umwelt nachhaltig schädigen.

Der Betreiber ist verpflichtet, elektrische und elektronische Geräte am Ende ihrer Lebensdauer an den Hersteller, die Verkaufsstelle oder an dafür eingerichtete, öffentliche Sammelstellen kostenlos zurückzugeben.

Entsorgung in Deutschland:
Die dormakaba EAD GmbH übernimmt nach Nutzungsbeendigung die ordnungsgemäße Entsorgung der gelieferten Ware entsprechend den gesetzlichen Regelungen (ElektroG-Gesetz in Deutschland). Anfallende Transportkosten ins Herstellerwerk sind vom Besitzer des Elektroaltgerätes zu tragen.

Entsorgung in der Schweiz:
Das Gerät ist einer Elektrogeräte-Rücknahmestelle entsprechend VREG zuzuführen.

In der EU sind Elektrogeräte nach den landesüblichen Entsorgungs- und Umweltrichtlinien zu entsorgen.

Löschung personenbezogener Daten

Für die Löschung personenbezogener Daten ist eigenverantwortlich Sorge zu tragen.

Verpackung umweltgerecht entsorgen.
Die Verpackungsmaterialien sind recyclebar. Bitte die Verpackungen nicht in den Hausmüll werfen, sondern einer Wiederverwertung zuführen.

Stichwortverzeichnis

T

U

V

W

Z

Notizen

04500551 - 07/2024

www.dormakaba.com

dormakaba Deutschland GmbH
Albertistraße 3
78056 Villingen-Schwenningen
Deutschland
T: +49 7720 603-0
www.dormakaba.com
Sitz der Gesellschaft: Ennepetal