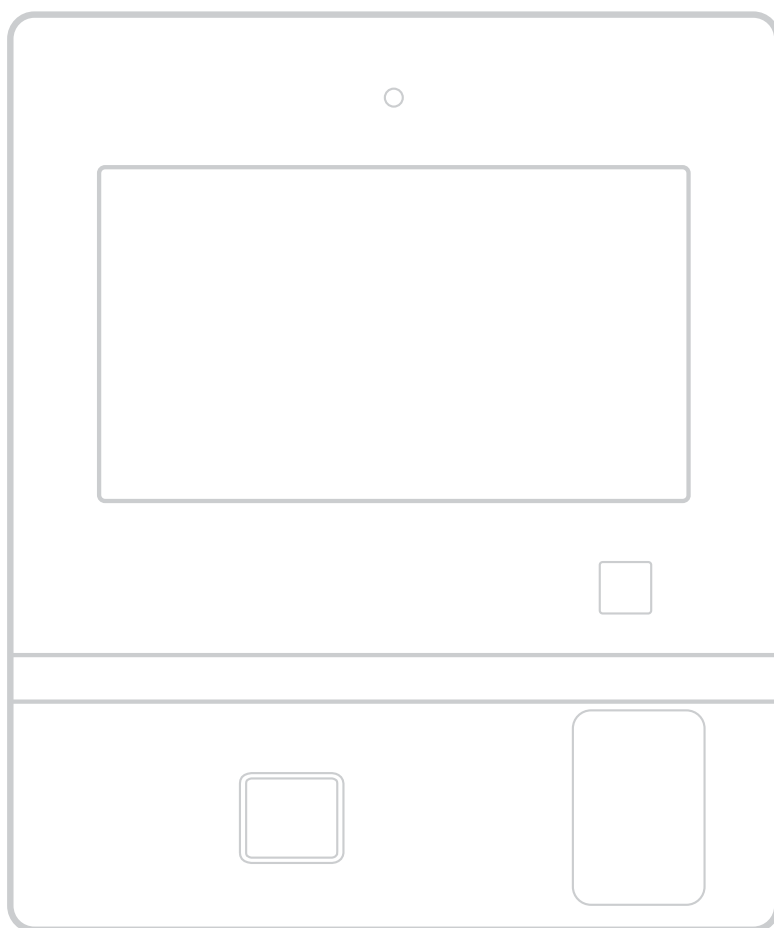


# Terminal ONE / Terminal 96 00

Technical Manual



# Table of Contents

<b>1</b>	<b>About this document</b>	<b>4</b>
1.1	Validity	4
1.2	Target Group	4
1.3	Contents and purpose	4
1.4	Warnings	5
	1.4.1 Hazard Categories	5
	1.4.2 Symbols	5
1.5	Notes	5
1.6	Action steps	5
<b>2</b>	<b>General safety instructions</b>	<b>6</b>
2.1	Intended use	6
2.2	Qualification of persons	6
2.3	Lithium battery	6
2.4	Mounting and installation	6
2.5	Accessories and spare parts	6
2.6	Service and maintenance	6
2.7	Data protection and IT security	7
<b>3</b>	<b>Product Description</b>	<b>8</b>
3.1	Overview	8
3.2	Technical Data	9
	3.2.1 System	9
	3.2.2 Power supply	9
	3.2.3 Interfaces	9
	3.2.4 Frequency bands and transmission power	9
	3.2.5 Inputs (IN1–IN2)	10
	3.2.6 Output (OUT)	10
	3.2.7 Reader	10
	3.2.8 Ambient conditions	10
	3.2.9 Dimensions	11
3.3	Conformity	12
3.4	Markings	13
3.5	Delivery contents	13
3.6	Accessories	14
	3.6.1 IP65 seal set	14
<b>4</b>	<b>Design and function</b>	<b>15</b>
4.1	Components	15
4.2	Front	15
4.3	Back	16
4.4	Variants	17
4.5	Overview of device software	18
	4.5.1 Service interface	19
<b>5</b>	<b>Installation</b>	<b>20</b>
5.1	Installation conditions	20
	5.1.1 Installation location	20
	5.1.2 Required cables and power supply	21
5.2	Screwing the mounting plate to the wall	22
5.3	Removing the cable cover	23
5.4	Inserting the cables into the device	24
5.5	Connections	25
	5.5.1 Connecting the network cable	25
	5.5.2 Connecting door components	26
	5.5.3 Connecting a USB component	27
5.6	Closing the cable cover	28
5.7	Close the IP65 cable cover	29

5.8	Mounting the terminal to the mounting plate	30
5.9	Remove the protective films	30
<b>6</b>	<b>Start-up</b>	<b>31</b>
6.1	LAN/WLAN requirements	31
6.2	Start of commissioning	32
6.3	Overview of manual commissioning	33
6.4	Android system settings	34
6.4.1	Accessing Android system settings	34
6.4.2	Changing network settings	35
6.4.3	Changing the volume	36
6.4.4	Activating voice output (text to speech)	37
6.5	Settings with the service interface	38
6.5.1	Accessing the service interface on the terminal	38
6.5.2	Accessing the service interface on the computer	38
6.5.3	Changing service interface password	39
6.5.4	Uploading and setting up a certificate with the service interface	40
6.5.5	Setting up an authentication procedure with the service interface	40
6.6	Automatic registration via B-COMM	41
6.7	Reader initialization	42
6.7.1	LEGIC	42
6.7.2	MIFARE (ARIOS)	43
6.7.3	MIFARE (Baltech)	43
<b>7</b>	<b>Operation</b>	<b>44</b>
7.1	Navigation buttons	44
7.2	Symbols for user guidance	45
7.2.1	Function buttons	45
7.2.2	Command prompt	45
7.2.3	Error states	46
7.2.4	CardLink	46
7.2.5	Finger input	47
7.3	Local enrollment: Managing fingerprints with the terminal	48
7.3.1	Accessing Local Enrollment	49
7.3.2	Enroll: Capturing a person's fingerprints	50
7.3.3	Unenroll: Deleting a finger template	51
<b>8</b>	<b>Cleaning the housing</b>	<b>52</b>
<b>9</b>	<b>Maintenance</b>	<b>53</b>
9.1	Maintenance overview	53
9.2	Updating the device software	54
9.3	RFID reader: Displaying the installed firmware version	55
9.4	RFID reader: Update firmware	55
9.5	Activating or deactivating the web server	56
9.6	Activating or deactivating the SSH server	56
9.7	Connecting the SSH client to the terminal	57
9.8	Activating a USB keyboard with an SSH client	57
9.9	Deactivating the USB keyboard with an SSH client	58
9.10	Accessing terminal files with an SFTP client	59
9.11	Displaying the functional scope of the license	60
9.12	Expanding the functional scope with a new license	61
9.13	Displaying system information	61
<b>10</b>	<b>Packaging/Return</b>	<b>62</b>
10.1	Complete Devices	62
10.2	Labelling	62
<b>11</b>	<b>Disposal</b>	<b>63</b>
	<b>Index</b>	<b>64</b>

# 1 About this document

## 1.1 Validity

This document describes the product:

Product name:	Terminal 96 00	Terminal ONE
Product code:	9600-K7	ONE-K7
Item number:	04579602	04579610
Device software:	772-00-X-K00	
BaseApp:	796-00-X-K00	
Test program:	739-00-X-K00	
Date of manufacture:	From April 2024	

This document describes all product variants and all optional features and functions. Options are chargeable and are therefore only available if they have been purchased. Additional features and functions may not be available at the time the document was written and can potentially be purchased at a later date.

## 1.2 Target Group

This document is aimed exclusively at professionals.

## 1.3 Contents and purpose

The contents is limited to the assembly, installation, start-up, and basic operation of the hardware.

## 1.4 Warnings

Warnings containing information/instructions and prohibitions to prevent injury to persons and damage to property are specially labeled.

Please pay attention to warnings. They are intended to help prevent accidents and avoid damage.

### 1.4.1 Hazard Categories

Warnings are split into the following categories:



#### CAUTION

##### Slight Risk

Describes a potentially hazardous situation that could result in minor physical injuries.



#### NOTICE

##### Information on how to handle the product correctly.

Failure to comply with these warnings may result in malfunctions. The product can be damaged.

### 1.4.2 Symbols

Depending on the source of the hazard, symbols are used for the warnings, and these have the following meanings:



General danger



Danger for electronic components from electrostatic discharge

## 1.5 Notes

Notes are marked with an info symbol.



Application tips and useful information

These tips help you to make optimal use of the product and its functions.

## 1.6 Action steps

The layout and symbols of the action steps are illustrated in the following example:

- ✓ Requirement
- 1. Step 1
  - ⇒ Intermediate result
- 2. Step 2
  - ⇒ Result

# 2 General safety instructions

Read and observe this document before using the device in order to avert personal injury and property damages.

## 2.1 Intended use

This device is intended for use as a terminal device for entering and displaying time registration, door control and employee communication data.

Any other use is not intended.

## 2.2 Qualification of persons

The actions described in this document must be performed by professionals. The professionals must be trained and authorized by dormakaba.

Professionals have attended appropriate technical training and acquired experience with the technology used. Professionals are responsible for compliance with the conditions specified by the manufacturer as well as applicable regulations and standards.

## 2.3 Lithium battery

The device contains 1 type CR2032 lithium battery as a backup battery.

- The battery does not require any service or maintenance work. The battery is designed to last until the end of the life cycle.
- Observe the safety regulations for the transportation of devices with lithium batteries.

## 2.4 Mounting and installation

- The device may be damaged due to transport/inappropriate storage.
  - Check the device for visible damage.
  - Do not put any damaged equipment into operation.
- The installation location must meet the climatic and technical conditions specified by the manufacturer.

## 2.5 Accessories and spare parts

- Only use components approved by dormakaba.
- Comply with the electrical specifications (voltage/power consumption).

## 2.6 Service and maintenance

- Modifications and changes to the device are not permitted.

## 2.7 Data protection and IT security

The device must be configured to ensure secure operation.

Without additional security settings, unauthorized access to the device and the system is possible.

### Security risks

- Violation of data protection through unauthorized access to personal data.
- Unauthorized access
- Tampering/system failure

### Recommended measures

- Device/service interface:
  - Change factory terminal password.
  - Change factory service interface password.
  - Keep device software up to date.
  - Replace factory SSH key file with a customer-specific SSH key file.
  - Deactivate SSH server after commissioning/maintenance.
  - Deactivate web server after commissioning/maintenance.
  - Before decommissioning: Reset the device to the factory settings.
- Browser (connection with service interface):
  - Do not save passwords in the browser.
  - Do not open any other websites in the browser while connected to the service interface.
  - Log out of the service interface before closing the browser.
  - Before closing the browser, clear the browser history.
- System software:
  - Activate encoded communication.
  - Install the latest patches.



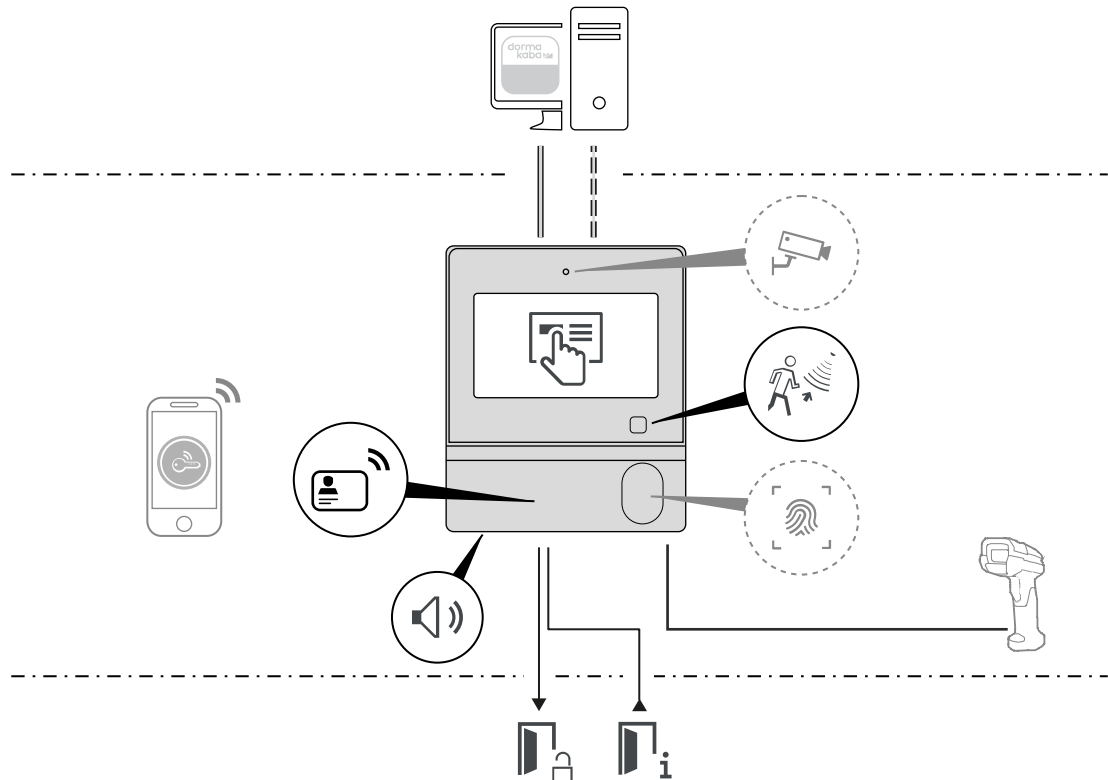
The recommended measures apply only to the device and do not claim to be complete or up to date.

The operator of the system must take appropriate measures to ensure the protection of personal data and IT security throughout their organization.

---

# 3 Product Description

## 3.1 Overview



The terminal can be used to capture time registration and employee communication data using RFID or biometrics. Interaction with the user takes place via the touch screen. The terminal can also be used as a door control for one door.

Depending on the configuration, users are identified with:

- RFID medium
  - The CardLink, AoC and DoC functions for writing data to RFID media are supported.
- Smartphone with Mobile Access app via Bluetooth®/NFC (optional)
- Fingerprint reader (optional)

The higher-level system software manages the system. Communication between the device and the system software can take place via:

- LAN
- WLAN

To reduce energy consumption, the terminal goes into standby mode after a period of inactivity. It is activated by a proximity sensor.

A camera may be integrated as an option.

A loudspeaker provides audible feedback.

The device has one output and two inputs for door control. An access control actuator can be controlled via the output. Door statuses can be captured via the inputs.

An additional device, such as a barcode scanner, can optionally be connected to the USB port.



## 3.2 Technical Data

### 3.2.1 System

#### Operating system

- Android 12

#### CPU

- i.MX8M Mini Quad processor

#### Memory

- 4 GB of DDR4 RAM
- 16 GB of eMMC flash memory

#### Display

- Type: TFT
- Size: 5.0"
- Resolution: 1,280 x 720 pixels (16:9 diagonal)
- Contrast: 1,200:1, typically 800:1
- Brightness: 430 – 500 cd/m<sup>2</sup>
- Lighting: LED
- Touch panel: capacitive

#### Audio

- Integrated loudspeaker (1 W)

### 3.2.2 Power supply

PoE according to IEEE802.3af (12.96 W)

### 3.2.3 Interfaces

- Ethernet: 10/100/1,000 Mbit/s
- USB: 2.0, socket type C

### 3.2.4 Frequency bands and transmission power

- 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 Inputs (IN1–IN2)

- For connection of potential-free contacts
- Integrated power supply: 5 V DC

### 3.2.6 Output (OUT)

- 1 change-over contact
- Contact rating: 30 V AC/DC; max. 2 A

### 3.2.7 Reader

Depending on the version, the following readers are supported:

#### **RFID reader**

- RFID chip: SM 6300
- Reading method:
  - 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 Energy/NFC)

#### **Fingerprint reader**

- Biometric Module (CBM) with integrated database for fingerprints.
- Optionally as CBM-E with extended approvals (PIV-IQS with FBI certification and FIPS 201-approved template evaluation)
- Storage capacity
  - ONE: 1,000 master records
  - 96 00: 50,000 master records

### 3.2.8 Ambient conditions

#### **Protection class according to IEC 60529**

- IP20
- IP65 if installation requirements are met.

#### **Relative humidity**

- 5–85%, non-condensing

#### **Ambient temperature**

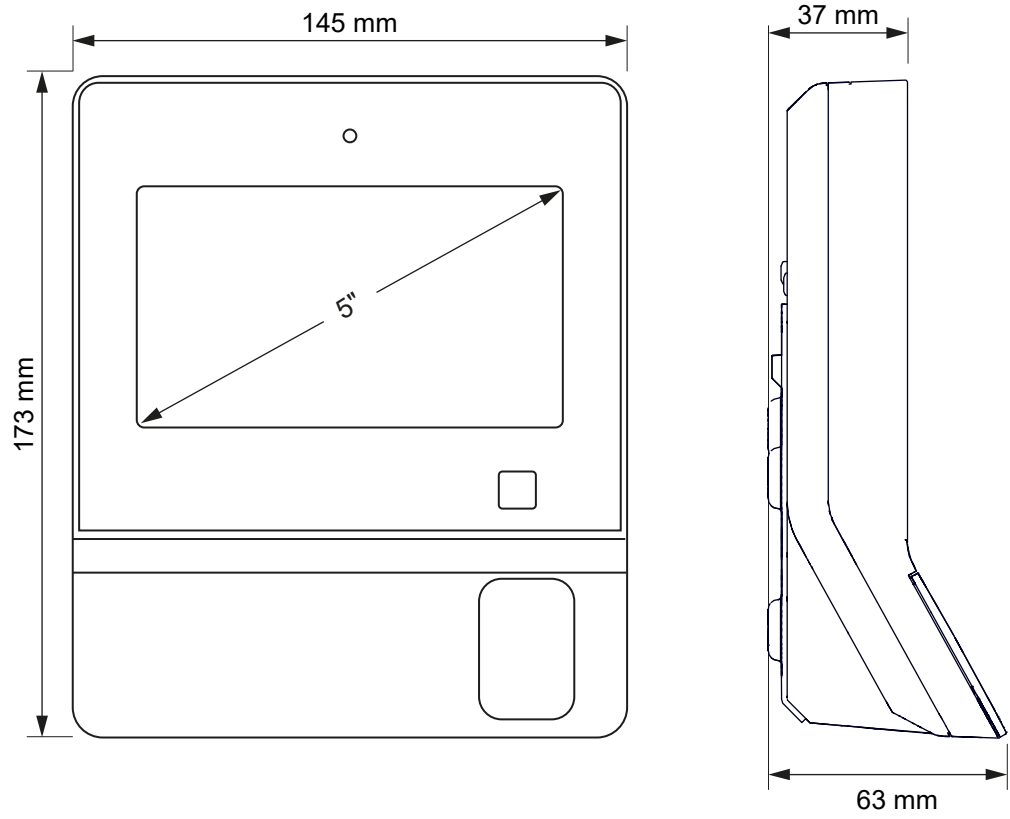
Environmental class 3K6:

- –25°C to +55°C (in use)
- –20 °C to +70 °C (in storage)

#### **Impact resistance**

- IK06

### 3.2.9 Dimensions



### 3.3 Conformity



This product complies with the provisions of EU directives:

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

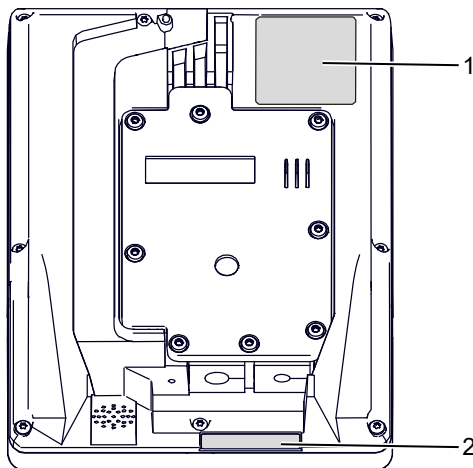
---

Full declarations of conformity are available online.

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

### 3.4 Markings

The product designation is located on the back of the terminal.



- 1 Type plate with the following content
  - Product name
  - Item number
  - Date of manufacture
  - Power supply data
  - Various symbols (conformity, safety and disposal)
- 2 Serial number

### 3.5 Delivery contents

- Terminal
- Mounting plate
- For wall mounting:
  - Screw 4.5 x 35 (x3)
  - Anchors (x3)
- For sealing the cable entries
  - Cable grommet 6 (x1)
  - Cable grommet plug 6 (x1)
  - Cable grommet 8 (x1)
  - Cable grommet plug 8 (x1)

## 3.6 Accessories

### 3.6.1 IP65 seal set

To achieve protection class IP65, additional parts are required.

- IP65 cable cover
  - 8 screws
- Cable grommets
  - Cable grommet 5 (x1)
  - Cable grommet 7 (x1)
  - Cable grommet 9 (x1)
  - Dummy grommet BTK (x1)

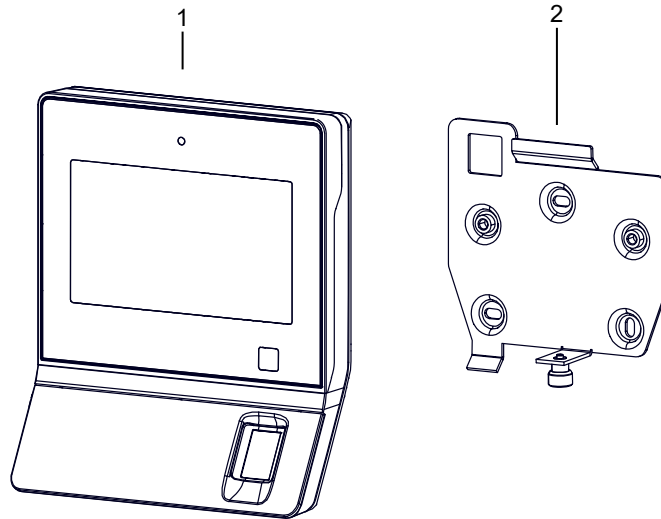
Order number: 04500555 (DE, VIS)

# 4 Design and function

## 4.1 Components



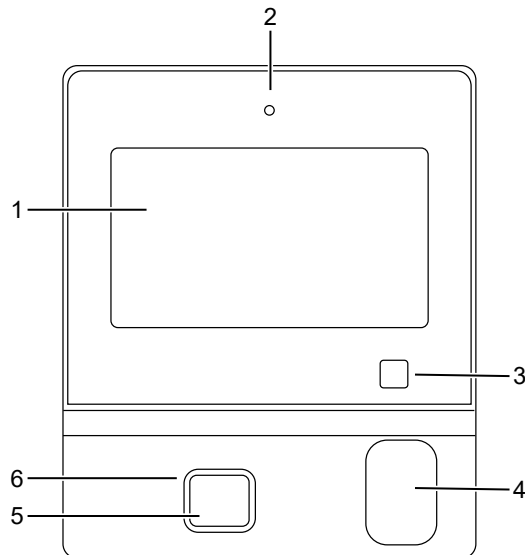
The terminal has a motion sensor for tamper detection. If the terminal is moved during operation, the device software generates an alarm record.



1 Terminal

2 Mounting plate

## 4.2 Front



1 Touch screen

3 Proximity sensor

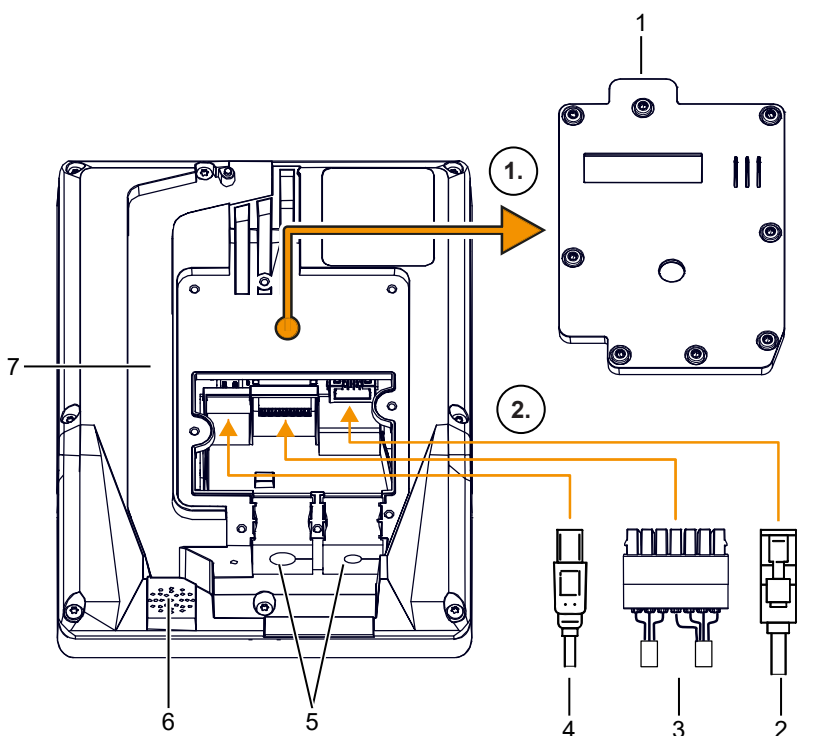
5 RFID reader

2 Camera (optional)

4 Fingerprint reader (optional)

6 Illuminated ring RFID reader

### 4.3 Back



- 1 IP20 cable cover
- 2 LAN port (RJ45)
- 3 Connection terminals for inputs/output
- 4 USB port (type C)
- 5 Cable grommets
- 6 Loudspeaker
- 7 Cable duct for cable routing from top to bottom



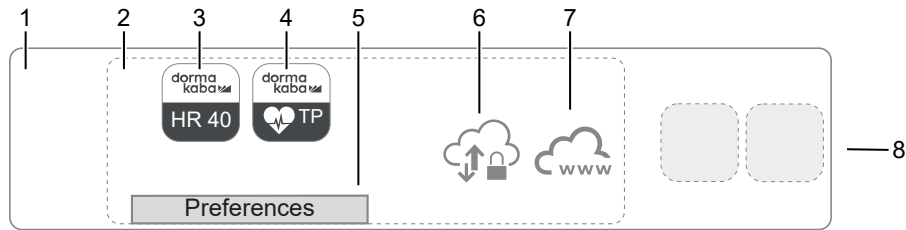
## 4.4 Variants

Outfitting	ONE	96 00		
		96 20	96 40	96 60
<b>Device software</b>				
B-Client HR40	●	●	●	●
<b>Reader</b>				
RFID reader, LEGIC/MIFARE (SM6300)	●	●	●	●
HID iClass SE/Prox	○	○	○	○
Fingerprint reader	○	○	○	○
<b>Interface (host)</b>				
Ethernet 10/100/1,000 (PoE)	●	●	●	●
WLAN	○	○	○	○
<b>Applications</b>				
Mobile Access	–	●	●	●
CardLink/Access on Card (AoC)	–	–	●	●
Door control	○	–	–	●
Loudspeaker	●	●	●	●
Energy-saving mode with proximity sensor	●	●	●	●
Camera	–	●	●	●
<b>Memory</b>				
1,000 master records	●	–	–	–
50,000 master records	–	●	●	●

### Legend

- Standard
- Optional
- No

## 4.5 Overview of device software



1 Operating system Android

### 2 BaseApp

The BaseApp is part of the basic configuration and is the platform for all apps on the terminal.

Important functions of the BaseApp:

- Protect the operating system from unauthorized access.
- Organize and start the apps.
- Provide functions and interfaces for accessing the hardware.
- Provide service functions for commissioning and maintaining the device.

### 3 B-Client HR40

Takes over the functions for time registration and door control.

For details, see reference manual of B-Client HR40

### 4 Test program

System settings: Configuration of the readers, service language

Tests: Reader, display, touch screen, inputs/outputs and sensors

Information display via the terminal

5 Preferences, depending on the call

- **Service interface** – local  
Provides functions for commissioning, operation and maintenance.
- **Android system settings**  
Provides functions for commissioning, operation and maintenance.

### 6 SSH server

- Enables remote access with an SFTP client.  
The terminal's file system can be accessed directly.
- Enables remote access to the terminal with an SSH client.  
Service functions can be executed using commands.

### 7 Web server

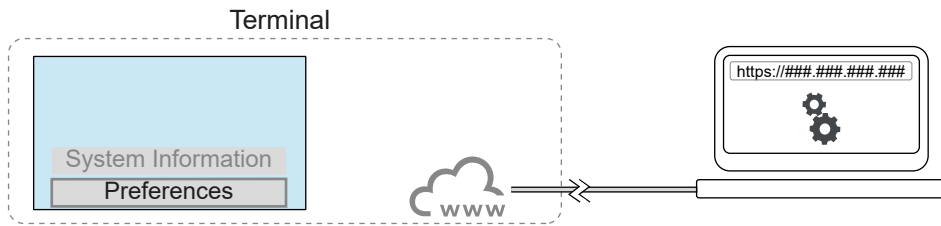
Enables remote access to the service interface with a browser.

8 Optional apps

Other apps can be installed if additional functions are required.

### 4.5.1 Service interface

Functions for commissioning, operation and maintenance are available via the service interface of the terminal.



There are two ways to access the service interface.

- Locally via the touch screen of the terminal
- Remote access via the browser of a computer

Login with user name (admin) and service interface password is required.

There are three areas.

#### 1 System

- Information  
Current information on hardware, device software, MAC address and IP address
- License  
Up-to-date information on the licensed functions.
- Diagnostics  
Log files can be displayed and downloaded.
- Administration  
Functions: reboot device (restart), disable service interface (deactivate web server), cold restart (device is reset to factory settings) and reset SSH key

#### 2 Settings

- Network
- Biometrics
- Date and time
- User administration
- Display management
- HR client

#### 3 Firmware

- Firmware download  
The firmware of the internal RFID reader can be updated.

# 5 Installation

## 5.1 Installation conditions

### 5.1.1 Installation location

- Install the device permanently in buildings. Installation in vehicles is not permitted.
- Only install the device in locations with ambient conditions suitable for the device.

#### **Avoid electromagnetic interference**

- Do not install the device in the vicinity of strong electromagnetic fields (possible sources of interference: switching power supplies, power lines etc.).

#### **Avoid radio interference**

- Maintain a distance of at least 20 cm from other RFID readers.
- Comply with the minimum distances from other mobile access components (Bluetooth). See Mobile Access planning guideline.

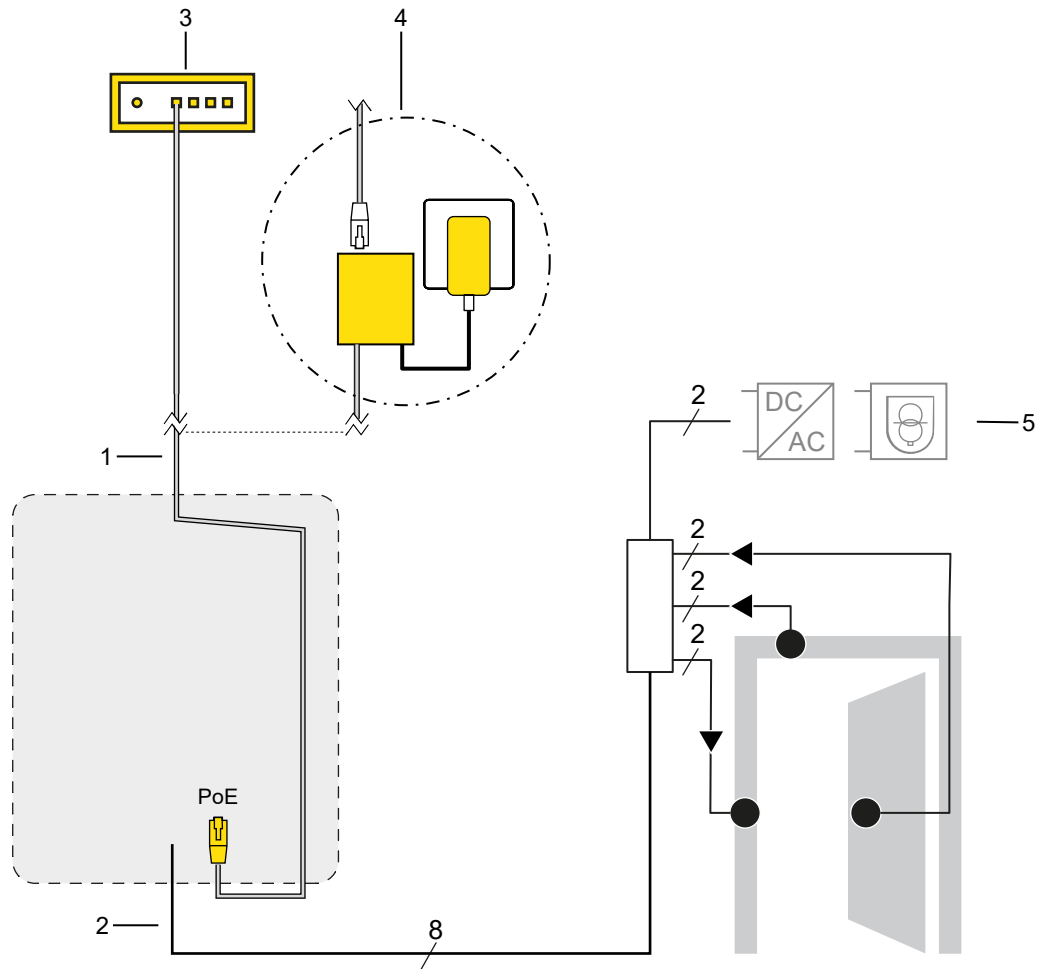
#### **Avoid overheating the device**

- Install the device at a sufficient distance from heat sources.
- Do not install the device in locations exposed to direct sunlight.

#### **WLAN/mobile radio**

- Before installation, check whether sufficient reception is guaranteed.

### 5.1.2 Required cables and power supply



#### Cables

- 1 LAN
  - at least CAT.5e, S/UTP
  - assembled with RJ45 plug
- 2 Cable to door components
  - Conductor cross-section: 0.14 to 0.5 mm<sup>2</sup>/AWG 26 to 20
  - Recommendation: J-Y(ST)Y 4X2X0.8

#### Power supply for device

- 3 PoE switch  
or
- 4 PoE injector

#### Power supply for door components

- 5 Power supply unit  
Power supply units must be compliant with IEC/EN/UL/CSA 62368-1.

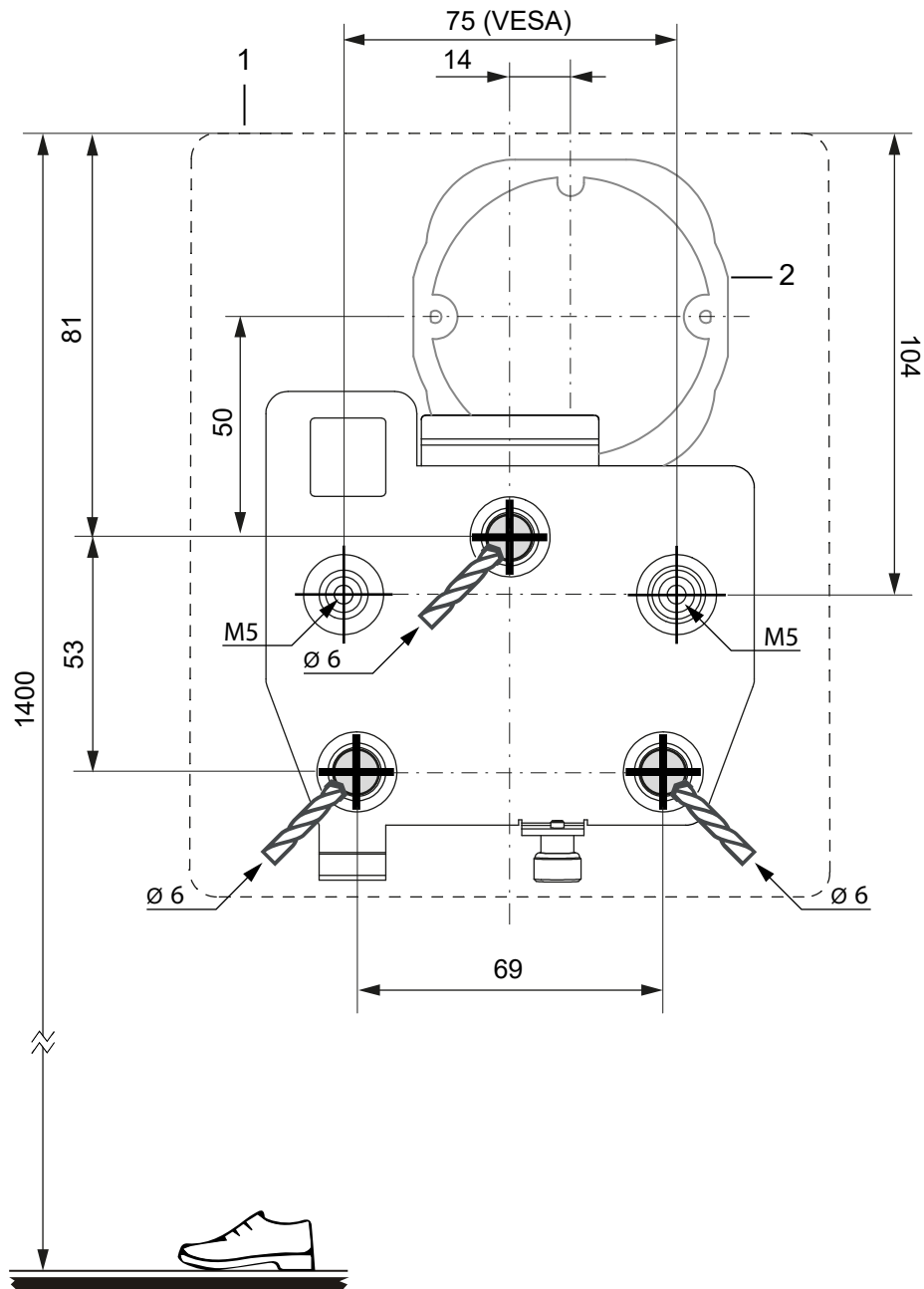
## 5.2 Screwing the mounting plate to the wall

Install the device at a suitable operating height for all users.

**Recommendation:** 140 cm from the finished floor to the top edge of the device.



Alternatively, the mounting plate can be screwed to a monitor mount (VESA MIS-D, 75 x 75 mm) using the M5 threads.



All dimensions in mm.

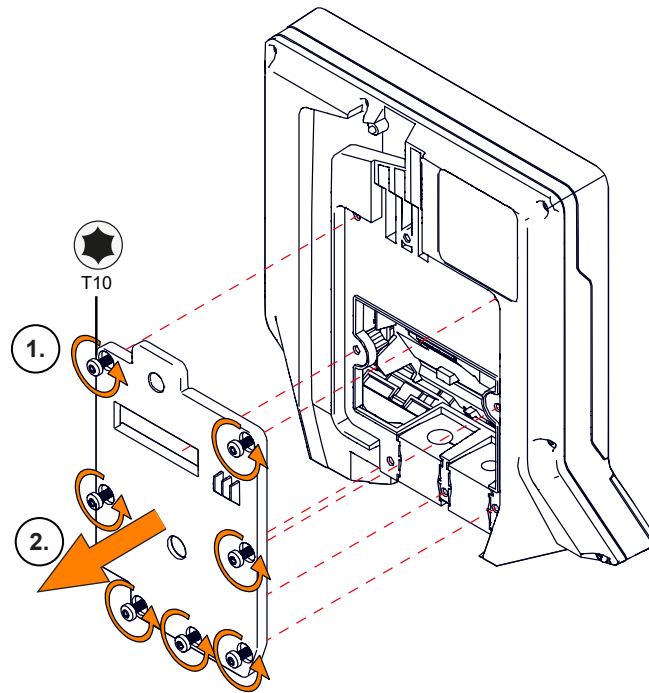
1 Device contour

2 Optional: flush-mounted device box for cables

1. Mark 3 drill holes on the wall.
2. Drill 3 holes in the wall.
3. Insert 3 anchors into the holes.
4. Position the mounting plate and screw down with the 3 screws.

### 5.3 Removing the cable cover

The connections are not accessible until the cable cover has been removed.



1. Loosen the 7 screws.
  2. Remove the cable cover.
- ⇒ The connections are accessible.

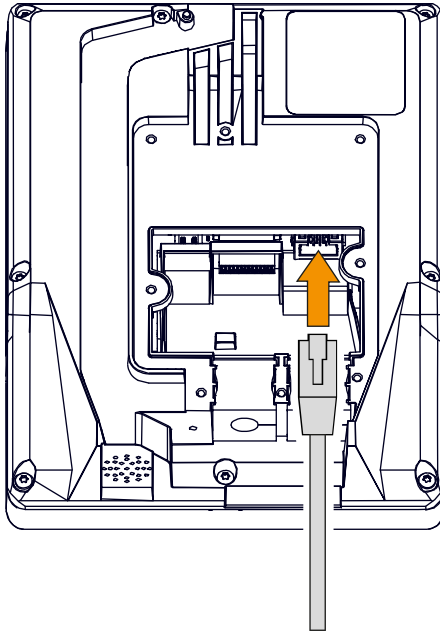




## 5.5 Connections

### 5.5.1 Connecting the network cable

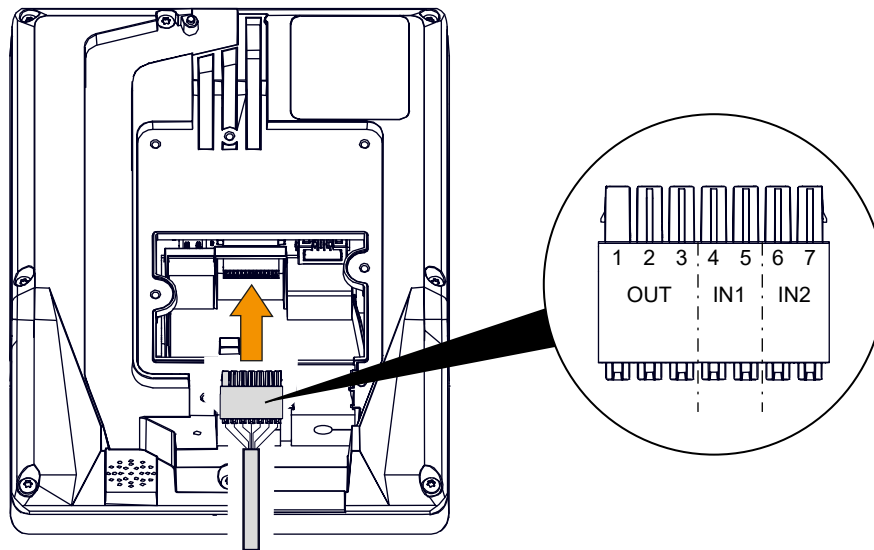
Remove the cable cover beforehand. See [Removing the cable cover](#) [▶ 5.3]



Plug the network cable into the RJ45 socket.

### 5.5.2 Connecting door components

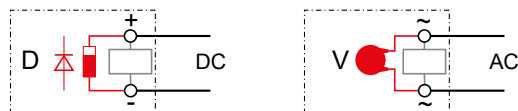
Remove the cable cover beforehand. See [Removing the cable cover \[► 5.3\]](#)



#### Output (OUT)

Terminal	Assignment	Wiring
1	C	
2	NO	
3	NC	

- Contact rating: 30 V AC/DC; max. 2 A
- Power supply units must be compliant with IEC/EN/UL/CSA 62368-1.
- If an inductive door component (door opener etc.) is not interference suppressed, suppress interference for the door component using one of the following measures:



- Direct voltage (DC): connect diode [D] in parallel in the reverse direction.
- Alternating voltage (AC): connect varistor [V] in parallel.

#### Inputs (IN1-IN2)

Terminal	Assignment	Wiring
4/6	GND	
5/7	IN1/IN2	

- Input is active when contact IN to GND is closed.

### 5.5.3 Connecting a USB component



The use of USB keyboards is deactivated by default.



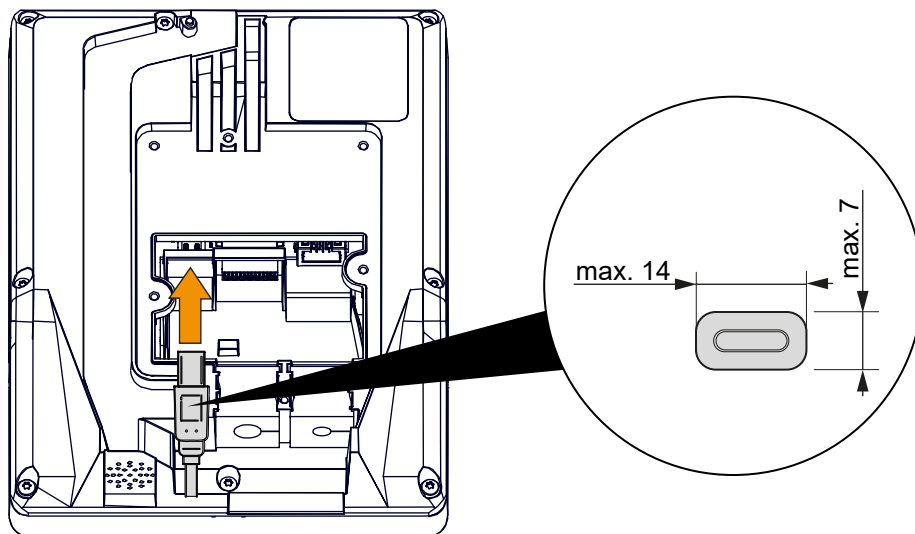
#### NOTICE

##### Use of unapproved barcode scanners

If barcode scanners are not obtained from dormakaba, proper functioning is not guaranteed.

- Only use barcode scanners approved by dormakaba.
- The barcode scanner must support a virtual COM port.

Remove the cable cover beforehand. See [Removing the cable cover](#) [▶ 5.3]

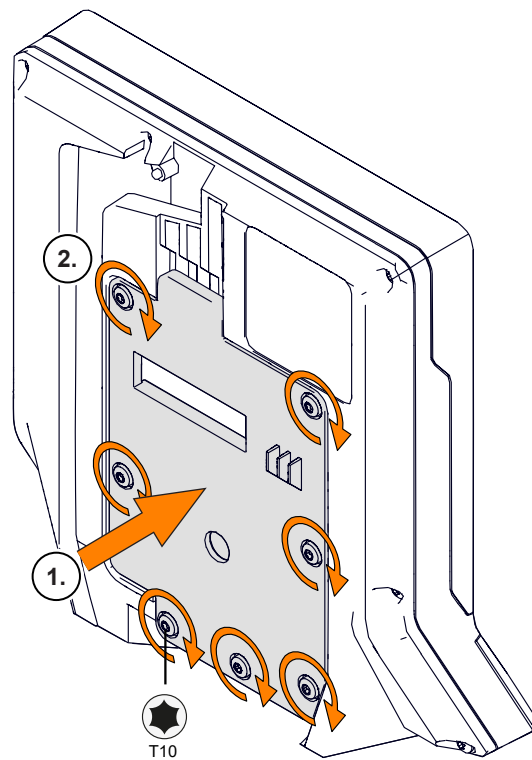


Plug the USB cable into the USB socket.

## 5.6 Closing the cable cover



With the original cable cover, the protection class is IP20.  
For protection class IP65, see [Close the IP65 cable cover](#) [▶ 5.7].

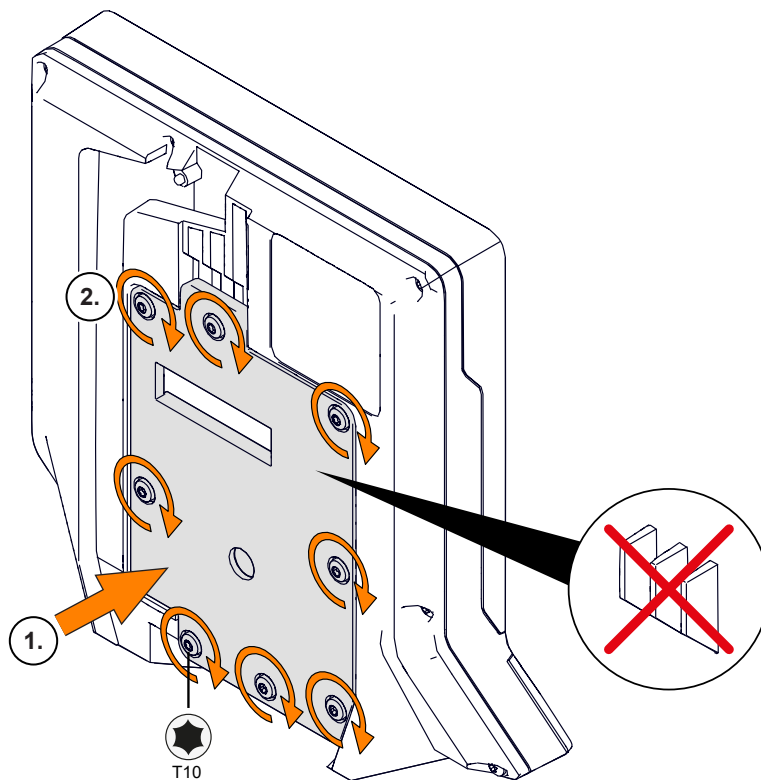


- ✓ The cables are connected.
- ✓ The cable grommets are plugged in.
- 1. Position the cable cover.
- 2. **Warning!**  
**If the screws are tightened too tightly or unevenly, the cable cover will bend.**  
Tighten the 7 screws.

## 5.7 Close the IP65 cable cover

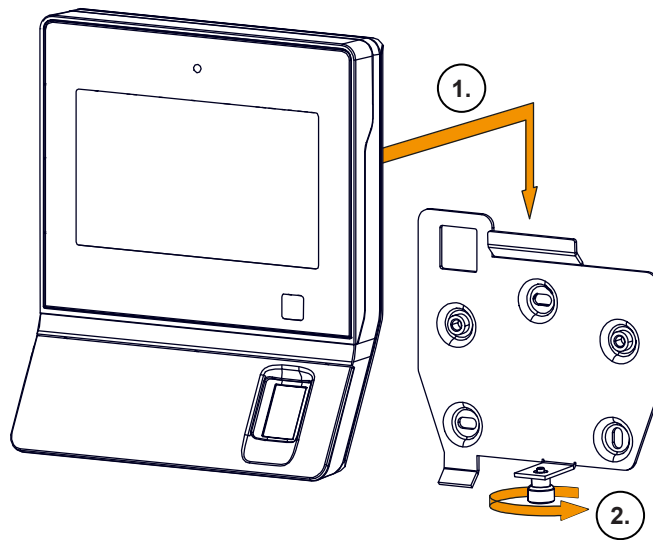


Use the cable cover from the IP65 seal set [[▶ 3.6.1](#)].



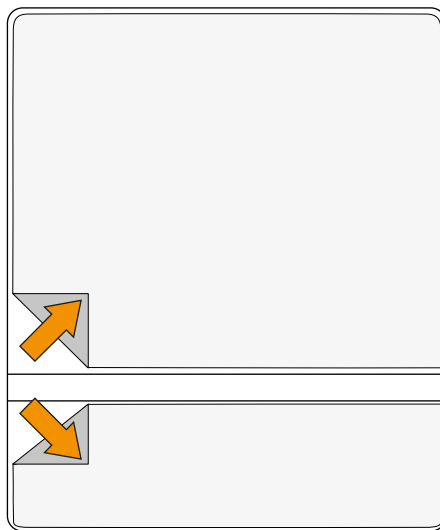
- ✓ The cables are connected.
- ✓ The cable grommets are plugged in.
- 1. Position the IP65 cable cover.
- 2. **Warning!**  
**The IP65 protection class has not been met due to loose screws. To prevent damage to the device:**  
Tighten the eight screws.

## 5.8 Mounting the terminal to the mounting plate



- ✓ The cable cover is closed.
- 1. Attach the terminal to the mounting plate.
- 2. Secure the terminal with the screw.

## 5.9 Remove the protective films



Remove the two protective films before commissioning.

# 6 Start-up

## 6.1 LAN/WLAN requirements

### Server

- A **DHCP server** is a prerequisite for:
  - Automatic assignment of the IP address (factory setting)
  - Automatic registration via B-COMM
- The SSDP service must be active in Windows Service Management.

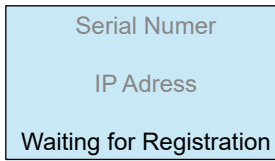
### Firewall

In the firewall, the following permissions must be granted.

Protocol/IP	Port		Usage
	Decimal	Hexadecimal	
UDP	Standard: 30464 Range: 30464 – 30703	7700 7700 – 77EF	Communication with system software
UDP	1900	76C	<ul style="list-style-type: none"> <li>• Automatic registration via B-COMM</li> <li>• MATRIX device scanner</li> </ul>
UDP/SSDP	30976	7900	Automatic registration via B-COMM
UDP	Standard: 30720 Range: 30720 – 30959	7800 7800 – 78EF	FTCS server
SSH/SFTP	22	16	SSH server
TCP	8443	20FB	Web server

## 6.2 Start of commissioning

As soon as the terminal is connected to the LAN and supplied with power via PoE, the terminal is in registration mode. In registration mode, the terminal can be registered automatically via B-COMM or put into operation with other system software.



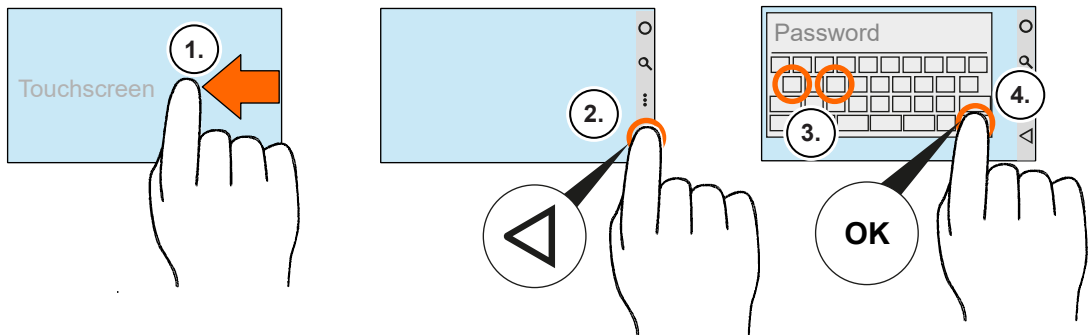
- The serial number of the terminal is displayed.
- The current IP address of the terminal is displayed. The default IP address is: 123.0.0.2



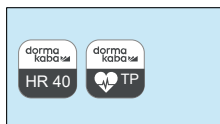
### Cancel the registration in the following cases.

- No DHCP server available on the network.
- A fixed IP address is to be used.
- IT security rules require authentication/certificates for the network.
- WLAN/mobile radio is to be used.

### Canceling registration



1. Swipe left.
  - ⇒ The navigation bar is displayed.
2. Touch and hold until the input mask is displayed.
3. Enter password.
  - Note:** For the first access, the password must be set.
4. Touch **OK**.
  - ⇒ Automatic registration is canceled.
  - ⇒ The BaseApp user interface is displayed.



- ⇒ Registration mode is exited.
- ⇒ Commissioning must be carried out manually.



### 6.3 Overview of manual commissioning

The table provides an overview of the settings which need to be made during commissioning and the options available.

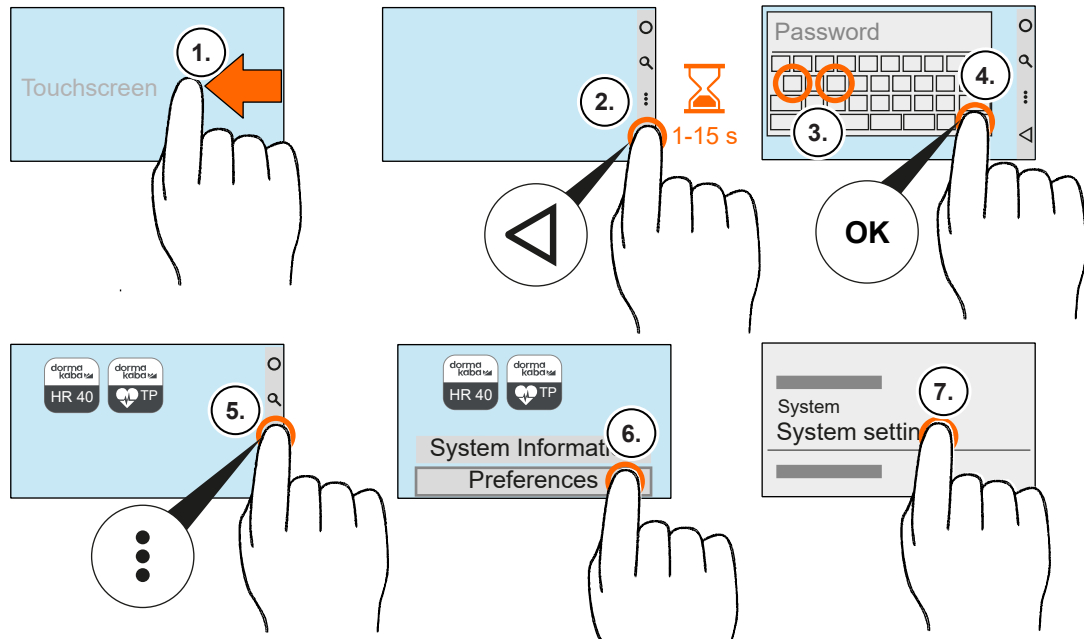
	Manual commissioning	Local			Remote access		
		Android-Systemeinstellungen	Testprogramm	Service Interface - lokal	Service Interface - Fernzugriff	SFTP-Client	Systemsoftware
1.	Change network settings. <ul style="list-style-type: none"> <li>IP protocol: IPv4 or IPv6</li> <li>Fixed IP address</li> </ul> If WLAN is to be used: <ul style="list-style-type: none"> <li>Establish WLAN connection.</li> </ul>	●	-	○	○	○	-
2.	If required by local IT security rules: <ul style="list-style-type: none"> <li>Set up certificate</li> <li>Set up authentication procedure</li> </ul>	○	-	-	●	○	-
3.	Change service interface password	-	-	●	●	○	○
4.	Initialize the RFID reader for the following reading methods: <ul style="list-style-type: none"> <li>LEGIC with AoC/DoC</li> <li>LEGIC with CardLink</li> <li>MIFARE Baltech</li> <li>MIFARE ARIOS</li> </ul>	-	-	-	-	-	-
		-	-	-	-	-	●



**Legend**

- Recommended
- Alternative
- Not possible

## 6.4 Android system settings

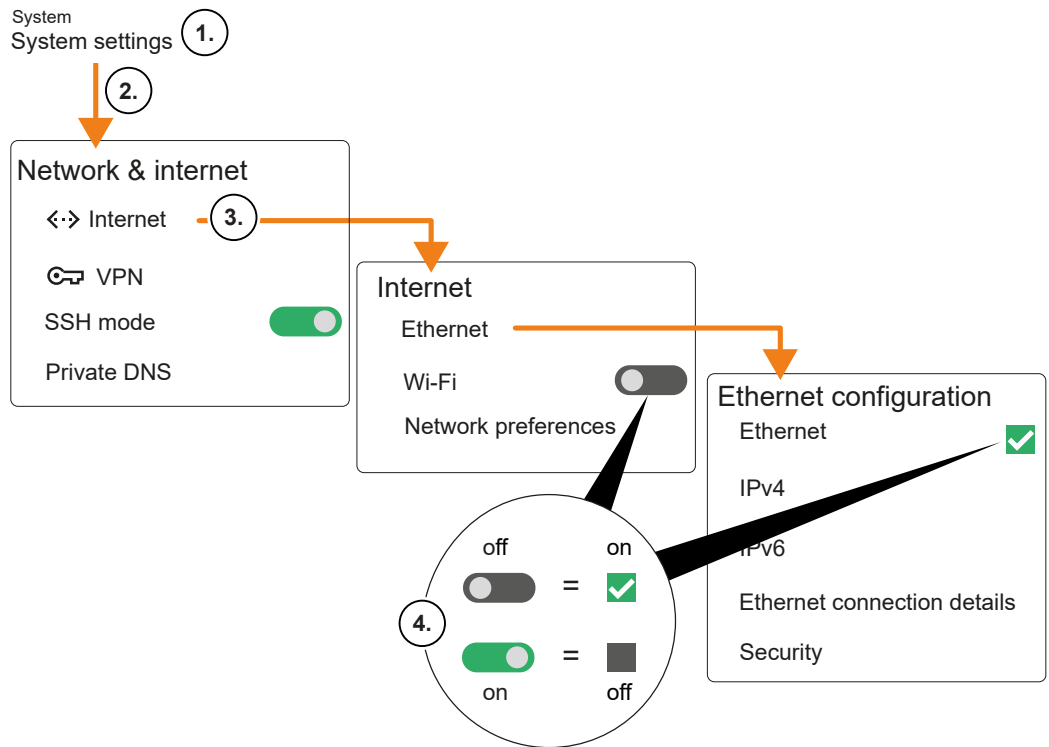
### 6.4.1 Accessing Android system settings



1. Swipe left.  
⇒ Navigation bar is displayed.
2. Touch and hold  until the input mask appears.  
**Note:** The duration can be set from 1 to 15 seconds. Default: 4 seconds
3. **Warning!**  
**The dialog is locked after three invalid password entries.**  
Enter password. (factory setting: admin)
4. Touch **OK**.  
⇒ HR client is exited. The BaseApp interface is displayed.
5. Touch .
6. Touch **Preferences** (settings).  
⇒ The Android settings open.
7. Touch **System setting**.

## 6.4.2 Changing network settings

- ✓ Accessing Android system settings [▶ 6.4.1]



1. Select **System settings**.
2. Select **Network & Internet**.
3. Select **Internet**.
4. Activate **Ethernet** or **Wi-Fi (WLAN)**.

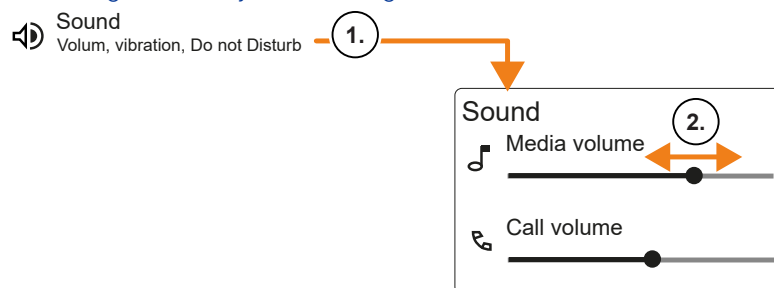
**Note:**

Activating/deactivating one network type activates/deactivates the other network type.

Ethernet (LAN)	Wi-Fi (WLAN)
<ol style="list-style-type: none"> <li>1 Select <b>IPv4</b> or <b>IPv6</b>.</li> <li>2 Select <b>Connection type</b>.                             <ul style="list-style-type: none"> <li>– Disable</li> <li>– DHCP</li> <li>– Static IP                                     <ul style="list-style-type: none"> <li>→ Enter IP address.</li> <li>→ Enter gateway.</li> <li>→ Enter netmask.</li> <li>→ Optionally, enter DNS1/DNS2.</li> </ul> </li> </ul> </li> <li>3 Confirm with <b>Done</b>.</li> </ol>	<ol style="list-style-type: none"> <li>1 Set <b>Wi-Fi</b> to <b>on</b>. ⇒ Available <b>Wi-Fi networks</b> are displayed.</li> <li>2 Select <b>Wi-Fi network</b>.</li> <li>3 Depending on the network: Enter the required information.</li> <li>4 Confirm with <b>Done</b>.</li> </ol>

### 6.4.3 Changing the volume

- ✓ Accessing Android system settings [[▶ 6.4.1](#)]



1. Select **Sound**.
2. Use the **Media volume** slider to adjust the volume.

### 6.4.4 Activating voice output (text to speech)

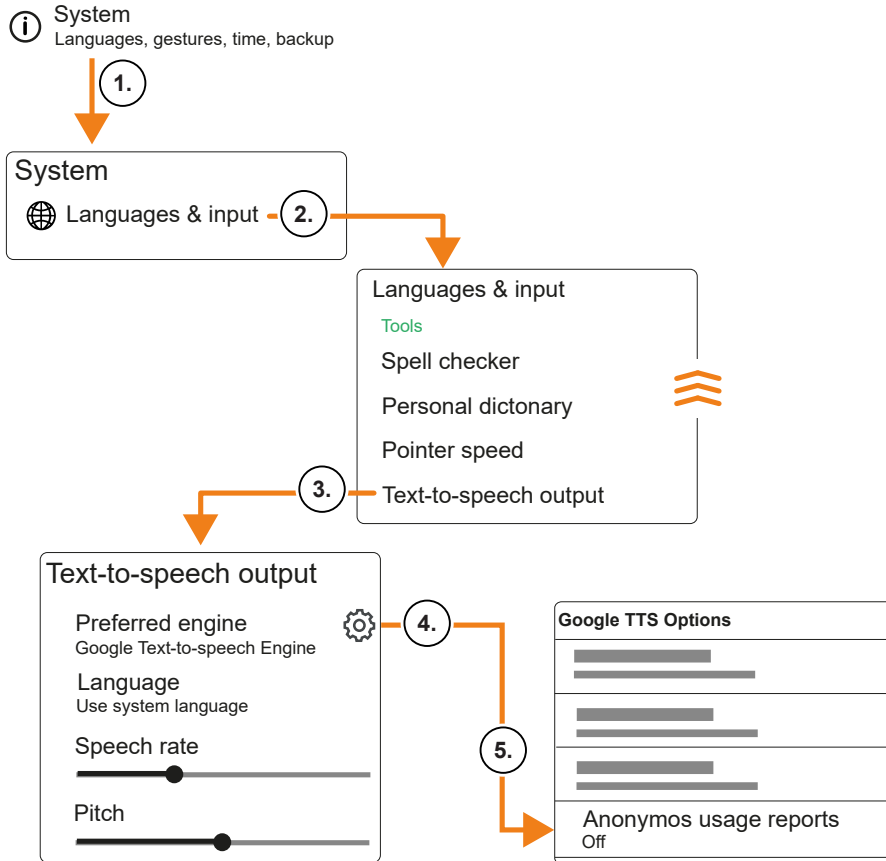
This function reads function button texts, dialog texts and booking responses out loud to the user.



Prerequisites for using this function:

- The function must be activated in the device software. See reference manual B-Client HR40.
- To download the language files, the terminal requires a one-time connection to the Internet.

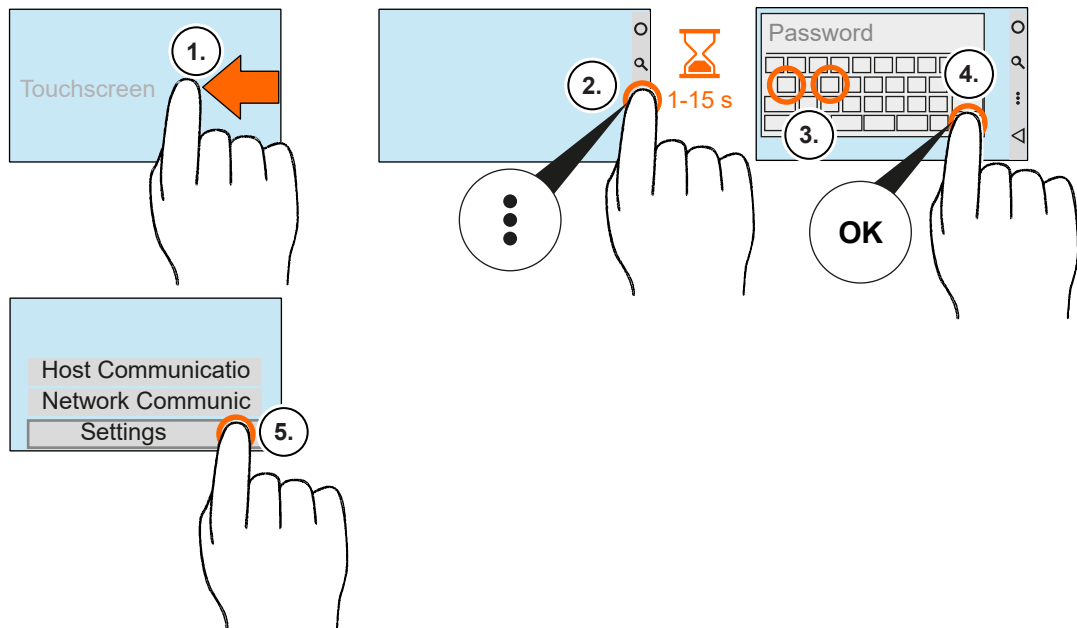
✓ [Accessing Android system settings](#) [▶ 6.4.1]



1. Select **System**.
2. Select **Languages & input**.
3. Select **Text-to-speech**.
4. Activate **Google Text-to-speech Engine** and accept warning message.
5. **Warning!**  
Data protection: Deactivate the collection of user data.  
Set **Anonymous usage reports** to **Off**.

## 6.5 Settings with the service interface

### 6.5.1 Accessing the service interface on the terminal



1. Swipe left.  
⇒ Navigation bar is displayed.
2. Touch and hold **⋮** until the input mask appears.  
**Note:** The duration can be set from 1 to 15 seconds. Default: 4 seconds
3. Enter password. (factory setting: admin)
4. Touch **OK**.
5. Touch **Settings**.  
⇒ The service interface is displayed.



The service interface is automatically closed after three minutes if no input is entered.

### 6.5.2 Accessing the service interface on the computer

- ✓ The IP address of the terminal is known.
  - ✓ The web server of the terminal is activated.
1. Open browser.
  2. Enter the IP address of the terminal on the address line. `https://###.###.###.###:8443`  
  
**If the browser warns you about an unknown certificate, confirm that the page is trustworthy.**  
⇒ The login window opens.
  3. Enter password. (factory setting: admin)
  4. Click **Log in**.  
⇒ The service interface is displayed.

### 6.5.3 Changing service interface password



#### NOTICE

**The factory password is widely known.**

To prevent unauthorized access:

- Change the factory password and use a secure password.



If the terminal is reset to the factory settings, the password will also be reset to the factory password.

- ✓ [Accessing the service interface on the computer \[▶ 6.5.2\]](#)  
[Accessing the service interface on the terminal \[▶ 6.5.1\]](#)
1. Select **User management** under Settings in the main menu.
    - ⇒ The **Change user passwords** dialog is displayed.
  2. Enter old password.
  3. Enter new password.
  4. Confirm new password.
  5. Touch **Submit**.
    - ⇒ The service interface password is changed.

## 6.5.4 Uploading and setting up a certificate with the service interface



This process is only possible via remote access.

- ✓ The certificate is stored locally on the computer.
- ✓ [Accessing the service interface on the computer](#) [▶ 6.5.2]
- 1. Select **Network** under Settings in the main menu.
  - ⇒ A dialog area with six tabs is displayed. Functions that are not supported are shown in gray.
- 2. Switch to the **Certificate management** tab.
- 3. Select **IEEE802.1x certificate**.  
(default: root certificate)
- 4. Enter **alias name** and **password** if required.
- 5. Upload certificate.
  - ⇒ In order for the certificates to be displayed, the page must be reloaded in the browser.
- 6. Change settings and touch **Submit**.
- 7. Go to **Administration** in the main menu and touch **Reboot**.
  - ⇒ The certificate is active after the restart.

## 6.5.5 Setting up an authentication procedure with the service interface



This process is only possible via remote access.

- ✓ [Accessing the service interface on the computer](#) [▶ 6.5.2]
- ✓ If a certificate is required for the authentication procedure, [Uploading and setting up a certificate with the service interface](#) [▶ 6.5.4]
- 1. Select **Network** under Settings in the main menu.
  - ⇒ A dialog area with six tabs is displayed. Functions that are not supported are shown in gray.
- 2. Switch to the **Network security** tab.
- 3. Select an authentication method and enter the required information.  
(default: None)
- 4. Touch **Submit**.
- 5. Go to **Administration** in the main menu and touch **Reboot**.
  - ⇒ The authentication procedure is active after the restart.



## 6.6 Automatic registration via B-COMM

Commissioning of the terminal is largely automated in conjunction with the B-COMM communication software.



The device is preset at the factory for automatic registration via B-COMM.

When communicating via WLAN, the connection must be set up and activated beforehand. This is done via the system settings.

---

### System requirements

- B-COMM communication software version 5.3.1.2 or higher
- IPv4-based network with a functioning DHCP server

### Commissioning procedure

1. Set up the power supply for the device.
  - ⇒ After system startup, the device reports cyclically to the B-COMMs which are active in the network.
  - ⇒ In this state, until commissioning is completed by a B-COMM, the message "**Waiting for registration**" appears in the display.
  - ⇒ If the device is detected by B-COMM, relevant data that identifies the device is queried.
  - ⇒ If the device is unknown, it is entered in B-COMM under the client B-COMM Terminal Discovery under the channel BCTDS (Terminal Discovery Stream).
2. Transfer device to the desired communication channel in B-COMM.
3. Provide device with the corresponding communication parameters.
  - ⇒ After the device has been permanently assigned in B-COMM, B-COMM first updates the device settings and saves them together with the "sop.ini" license file.
  - ⇒ The device now informs the B-COMMs active on the network that the registration has been completed, after which the device is removed from the BCTDS channel by other B-COMMs.
4. Load specific parameters and master records onto the device.
  - ⇒ The device software is restarted automatically. After that, the device is ready for operation.

## 6.7 Reader initialization

Some RFID readers must be initialized during initial commissioning.

### 6.7.1 LEGIC

For LEGIC readers, a reader initiation is required in certain cases:

- If a read-protected segment is to be used.
- If a write-protected segment is to be written, e.g. for CardLink applications.

#### Initiation of the reader

- ✓ A SAM 63 card (security card C2) with the corresponding segment area is required to initiate the reader.
1. Hold up the SAM 63 card when the device expects RFID input during normal operation.
    - ⇒ The start of the process is confirmed by an audible signal.
    - ⇒ Three consecutive audible signals are emitted if the process cannot be carried out, for example if the reader has already been initiated.
  2. The SAM 63 card must be in the reading field for about 15 to 20 seconds without interruption.
    - ⇒ Following successful initiation, three short audible signals are emitted.
    - ⇒ Eight consecutive audible signals are emitted if an error has occurred.
  3. Remove the SAM 63 card from the field.

#### Uninitiation of the reader

- ✓ The reader is uninitiated with a SAM 64 card.
1. Hold up the SAM 64 card when the device expects RFID input during normal operation.
    - ⇒ The start of the process is confirmed by an audible signal.
    - ⇒ Three consecutive audible signals are emitted if the process cannot be carried out, for example if the reader has already been uninitiated.
  2. The SAM 64 card must be in the reading field for about 15 to 20 seconds without interruption.
    - ⇒ Following successful uninitiation, three short audible signals are emitted.
    - ⇒ Eight consecutive audible signals are emitted if an error has occurred.
  3. Remove the SAM 64 card from the field.

### 6.7.2 MIFARE (ARIOS)

In systems with the ARIOS safety concept, the system key (a.k.a. sitekey) must be distributed to the individual readers.

The system key can be distributed in two ways.

- System key distribution via B-COMM.
- System key distribution via programming master A or B.

Details can be found in the reference manual for the device software.

### 6.7.3 MIFARE (Baltech)

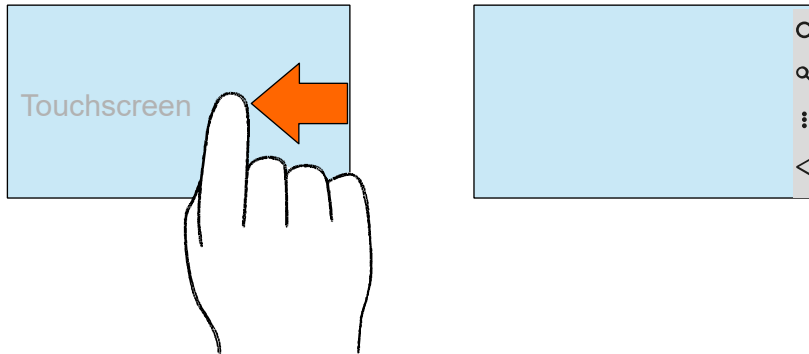
The MIFARE reader must be activated with a MIFARE configuration card:

1. Switch off device.
2. Switch on device.
3. Hold MIFARE configuration card up to the reader for approx. 10 seconds.

# 7 Operation

## 7.1 Navigation buttons

Swiping from the right edge of the display to the left displays the navigation bar. The navigation bar contains the Android navigation buttons.



The following functions are executed by touching the individual symbols:

- Home**  
Touching the home symbol takes you to the desktop view (start screen) of the device. As Android is capable of multitasking, the active programs continue running in the background.
- 🔍 Search**  
Touching the search symbol displays the search function for the active program.
- ⋮ Menu**  
Touching the menu symbol displays a menu with options for the current program or the current screen display.
- ◀ Back**  
By touching the back symbol, you can return to the last display view, e.g. from the submenu to the main menu.

If the system is expecting input, a virtual keyboard is shown in the display. In this input mode, the back symbol points downwards. Touching the back symbol exits input mode and hides the virtual keyboard.



The Home button and the Search button have no function within the B-Client device software, the test program and the BaseApp.

## 7.2 Symbols for user guidance

The following standard symbols are available to the device software for user guidance. The symbols are part of the BaseApp.



Display content, functions and operating sequences depend on the device software settings.

### 7.2.1 Function buttons

Examples of function button symbols. Other variants and symbols for additional functions are available.



Coming



Going



Business trips



Query



Special function

### 7.2.2 Command prompt

The following symbols indicate to the user which input is currently expected.



ID card entry via the RFID reader is expected.



Entry of an RFID ID card with biometric segment for biometric verification is expected.



Finger input via the biometric reader is expected.



ID or PIN input via the keypad is expected.

Depending on the system configuration, several alternative entries are possible. In this case, several symbols for the possible input types are displayed simultaneously.

### 7.2.3 Error states

The following symbols indicate error states to the user during a booking.



Invalid biometric verification

No biometric segment recognized on the ID card, or error when reading the finger template.



Invalid biometric verification

Fingerprint is not identical to the finger template on the ID card, or finger template does not exist.



Invalid biometric identification

There are no finger templates in the CBM reader database (database empty).



Invalid biometric identification

Fingerprint is not contained in the database.



Read error



Incorrect input via the keypad

### 7.2.4 CardLink

The following symbols are relevant when using the optional CardLink function.



A CardLink update is available.



An error occurred during CardLink validation or CardLink update.

### 7.2.5 Finger input

While the fingerprint is being scanned, the biometric reader provides event-driven user guidance.

The following symbols are shown in the display to indicate error statuses to the user.



Finger must be moved further to the left.



Finger must be moved further to the right.



Finger must be moved further up.



Finger must be moved further down.



Press finger more firmly.



Latent finger

Clean reading window of the biometric reader.



There are no finger templates in the CBM reader database (database empty).

This status is displayed immediately after the reader is activated.

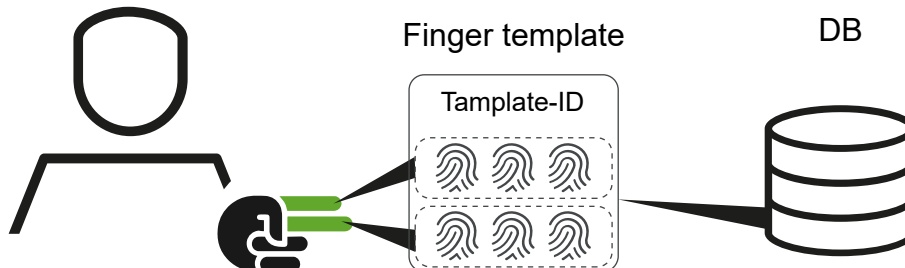
## 7.3 Local enrollment: Managing fingerprints with the terminal



Prerequisites for using the **Local Enrollment** function:

- The terminal has a fingerprint reader.
- The function is licensed.  
[Displaying the functional scope of the license](#) [▶ 9.11]

Fingerprints are captured with the internal fingerprint reader and saved in the fingerprint reader's internal memory.



For each person, two fingers are recorded with three prints each. Together with the template ID, the prints are saved in the database as a finger template.

There are two operating modes.

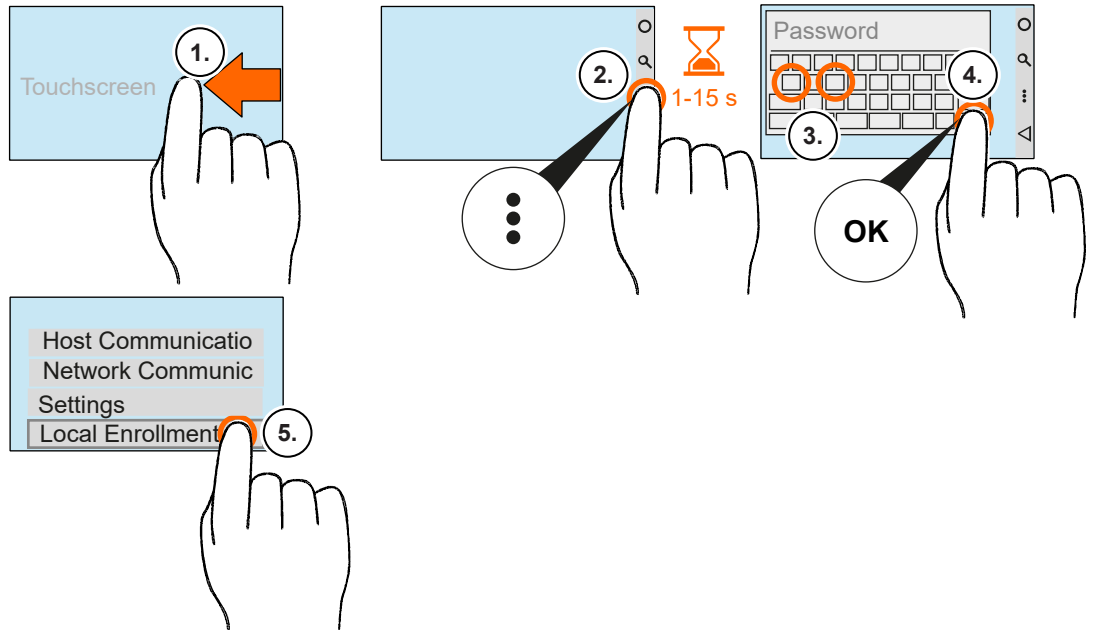
- **With biometric software**
  - The fingerprints are synchronized with the Finger Template Control Service (FTCS) and are available across the system.
  - An FTCS connection via the BCFTC channel is required to capture fingerprints (enroll).
- **Stand-alone**
  - Only the locally captured fingerprints are available.

There are five sub-functions.

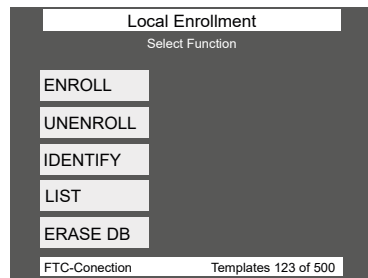
- 1 **ENROLL**  
[Enroll: Capturing a person's fingerprints](#) [▶ 7.3.2]
- 2 **UNENROLL**  
[Unenroll: Deleting a finger template](#) [▶ 7.3.3]
- 3 **IDENTIFY**  
 Displays the template ID of a person if the fingerprints have already been captured. The person must place a saved finger on the fingerprint reader.
- 4 **LIST**  
 Displays all template IDs saved in the database. The function is only available if fewer than 100 template IDs are saved.
- 5 **ERASE DB**  
 Deletes all saved finger templates from the database. The process is protected by the erase PIN, **439235**.



### 7.3.1 Accessing Local Enrollment



1. Swipe left.  
⇒ Navigation bar is displayed.
2. Touch and hold **⋮** until the input mask is displayed.  
**Note:** The duration can be set from 1 to 15 seconds. Default: 4 seconds
3. **Warning!**  
**The dialog is locked after three invalid password entries.**  
Enter password. (factory setting: admin)
4. Touch **OK**.
5. Touch **Local Enrollment**.  
⇒ The main window of **Local Enrollment** is displayed.



### 7.3.2 Enroll: Capturing a person's fingerprints

✓ Accessing Local Enrollment [▶ 7.3.1]

1. Select **Enroll**.
2. Enter **template ID**.

**Note**

The template ID is used to identify the person. The length of the template ID is specified by the **PresetEnroll** parameter.

3. Touch **OK**.  
⇒ A new window is displayed.
4. Record two fingers of the person three times each.

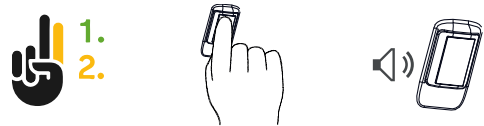
A quality value is specified for each recording process.

Above 120 = very good      60 to 120 = good      Below 60 = bad

1. Place first finger on the fingerprint reader and remove it after the signal tone.



1. Place first finger on the fingerprint reader and remove it after the signal tone.



1. Place first finger on the fingerprint reader and remove it after the signal tone.



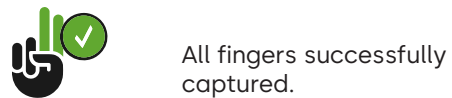
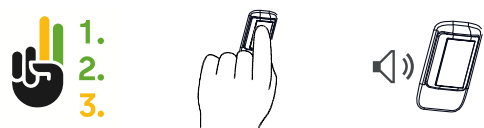
2. Place second finger on the fingerprint reader and remove it after the signal tone.



2. Place second finger on the fingerprint reader and remove it after the signal tone.



2. Place second finger on the fingerprint reader and remove it after the signal tone.



If the quality of a finger is poor, repeat the process.  
 If the quality of one finger is repeatedly poor, capture another finger.

5. Save the template.  
⇒ The person's fingerprints have been captured.

### 7.3.3 Unenroll: Deleting a finger template

✓ [Accessing Local Enrollment](#) [▶ 7.3.1]

1. Select **Unenroll**.
2. Select **finger template** via
  - **Numpad**  
Enter the template ID using the virtual keypad.
  - **Reader**  
Have the person place a captured finger on the fingerprint reader.
  - **List**  
The template ID is selected from the list.

# 8 Cleaning the housing

To clean the housing, use a soft, lint-free cloth and a mild window cleaning agent!



## NOTICE

### **Damage to the housing due to unsuitable cleaning agents**

To avoid damaging the housing during the cleaning process, please note the following:

- Do not use alcohol such as ethanol or isopropanol
  - Do not use harsh solvents
  - Do not use cleaning agents with powder additives
  - Avoid scratching and abrasive movements
-

# 9 Maintenance

## 9.1 Maintenance overview

The table provides an overview of possible maintenance tasks and the options available.

Maintenance task	Local			Remote access				
	Android-Systemeinstellungen	Testprogramm	Service Interface - lokal	Service Interface - Fernzugriff	SFTP-Client	SFTP-Installer	SSH-Client	Systemsoftware
Updating the device software [▶ 9.2]	-	-	-	-	-	●	-	-
RFID reader: Displaying the installed firmware version [▶ 9.3]	-	●	-	-	-	-	-	-
RFID reader: Update firmware [▶ 9.4]	-	-	-	●	-	-	-	-
Activating or deactivating the web server [▶ 9.5]	●	-	-	-	○	-	-	○
Activating or deactivating the SSH server [▶ 9.6]	●	-	-	-	○	-	-	○
Change terminal password	-	-	-	-	○	-	-	●
Unlock terminal password	-	-	-	-	○	-	-	●
Changing service interface password [▶ 6.5.3]	-	-	●	●	○	-	-	-
Activating a USB keyboard with an SSH client [▶ 9.8]	-	-	-	-	-	-	●	-
Deactivating the USB keyboard with an SSH client [▶ 9.9]	-	-	-	-	-	-	●	-
Displaying the functional scope of the license [▶ 9.11]	-	-	●	●	-	-	-	-
Expanding the functional scope with a new license [▶ 9.12]	-	-	-	-	-	●	-	-
Displaying system information [▶ 9.13]	○	-	●	●	-	-	-	-
Provide diagnostic data for support	-	-	-	●	-	-	-	-

### Legend

- Recommended
- Alternative
- Not possible

## 9.2 Updating the device software



Firmware, device software and other software are available in the **my.dormakaba portal**.  
<https://portal-dormakaba.onelogin.com>

---

The device software is updated with the **SFTP installer**.

Device software, apps and SFTP installer are provided as a ZIP file. Should there be a new Android version, it is also included.

The process distinguishes between an **update** and an **installation**.

- **Update**

The device software is updated to a new version. Current settings are retained.

- **Installation**

The device software is reinstalled. Current settings are lost, and the terminal must be recommissioned. This can be used to repair a faulty installation.

- ✓ SSH server of the terminal is activated.  
[Activating or deactivating the SSH server](#) [▶ 9.6]
- ✓ SFTP installer has been downloaded.
- ✓ For installation only: Device configuration and parameterization are saved.
- ✓ If there are customer-specific layout adjustments, the **interface.ini** file and corresponding images can be downloaded from the terminal and saved.

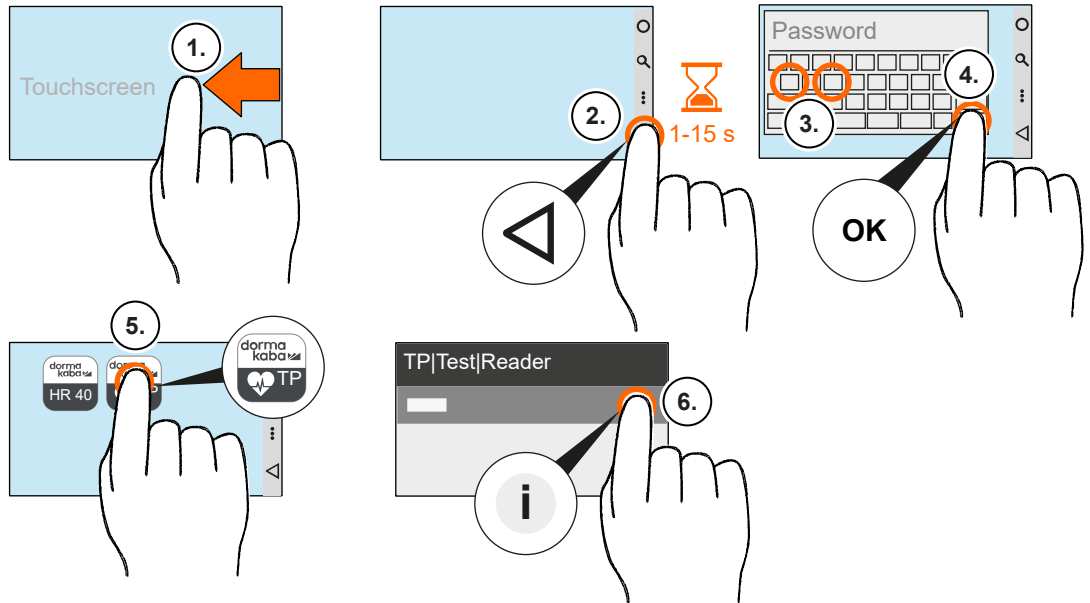
1. Unzip the SFTP installer (ZIP file) into a directory on the computer.
2. If the SSH key file has been changed, copy the customer-specific SSH key file to the unpacked directory.
3. Double-click **SFTP Installer.exe**.

**If a security warning is displayed, click Execute.**

⇒ SFTP Installer is opened.

4. Follow the instructions in the user interface.
  5. Restart the terminal.
- ⇒ The device software has been updated.

### 9.3 RFID reader: Displaying the installed firmware version



1. Swipe left.  
⇒ Navigation bar is displayed.
2. Touch and hold ◀ until the input mask appears.  
**Note:** The duration can be set from 1 to 15 seconds. Default: 4 seconds
3. **Warning!**  
**The dialog is locked after three invalid password entries.**  
Enter password. (factory setting: admin)
4. Touch **OK**.
5. Touch ⋮.
6. Touch **TP** (test program).  
⇒ The test program is opened.
7. Touch **Test/Reader**.
8. Touch **Info**.  
⇒ The installed firmware version is displayed.

### 9.4 RFID reader: Update firmware



Firmware, device software and other software are available in the **my.dormakaba portal**.  
<https://portal-dormakaba.onelogin.com>

- ✓ The terminal's web server is switched on.  
[Activating or deactivating the web server \[▶ 9.5\]](#)
  - ✓ RFID reader firmware is saved on the computer.
  - ✓ Service interface is accessed on the computer.  
[see [Accessing the service interface on the computer \[▶ 6.5.2\]](#)]
1. Select **Firmware update** under FIRMWARE in the main menu.  
⇒ The dialog area is displayed.
  2. Select the firmware file.
  3. Click **Start update**.

## 9.5 Activating or deactivating the web server



### NOTICE

#### IT security risk due to activated web server.

Unauthorized access to the terminal is possible via the web server.

- Deactivate web server after commissioning/maintenance.

The service interface is only available if the web server is activated.

✓ [Accessing Android system settings \[▶ 6.4.1\]](#)

1. Navigate to **Service Interface**.
2. Activate or deactivate web server.
  - ⇒  Web server deactivated
  - ⇒  Web server activated

## 9.6 Activating or deactivating the SSH server



### NOTICE

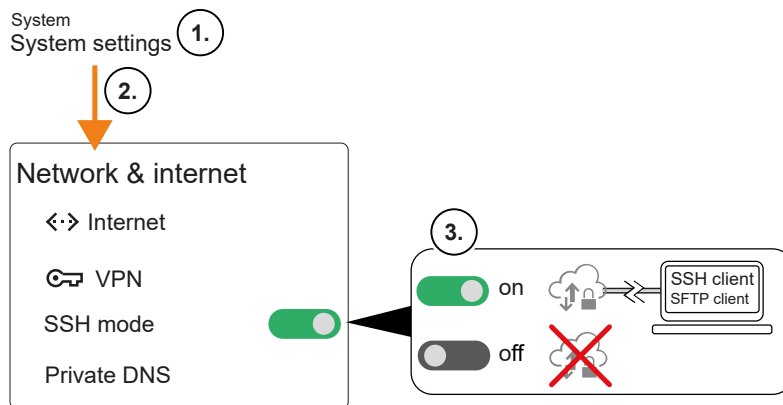
#### IT security risk due to activated SSH server.

Unauthorized access to the terminal is possible via the SSH server.

- Deactivate SSH server after commissioning/maintenance.

Access with an SFTP client or SSH client is only possible if the SSH server is activated.

✓ [Accessing Android system settings \[▶ 6.4.1\]](#)



1. Select **System settings**.
2. Select **Network & Internet**.
3. Switch **SSH mode** on or off.



## 9.7 Connecting the SSH client to the terminal

- ✓ **SSH client** (e.g. PuTTY) is installed on the computer.
  - ✓ **SSH server** on the terminal is activated.  
[Activating or deactivating the SSH server \[▶ 9.6\]](#)
  - ✓ **SSH key file** is available.  
 Default: kaba-private-ssh-key.ppk; if SSH key file has been changed, use the customer-specific SSH key file.
1. Start SSH client.
  2. Set up connection.

Setting	Value
Connection type	SSH/Telnet
Server address	<IPv4 address of the terminal>
Port	22
User name	root
password	kaba
Connection → SSH → AUTH → Credentials → Private key file	<Path to the SSH key file>

3. Click **Open**.  
 ⇒ The command window is displayed.
4. Enter **root** as login.
5. Enter **passphrase** (**kaba** or customer-specific).  
 ⇒ Terminal commands can be executed.

## 9.8 Activating a USB keyboard with an SSH client

The use of USB keyboards is deactivated by default.



### NOTICE

**If the use of USB keyboards is activated, unauthorized access to the system settings is possible via a USB keyboard.**

Only activate the USB keyboard briefly for service work.

- ✓ USB keyboard is not plugged in to the USB port.
  - ✓ [Connecting the SSH client to the terminal \[▶ 9.7\]](#)
1. Enter the command `setprop kdb.input.device.disable 0` and confirm with **Enter**.
  2. (Check setting.)  
 Enter the command `getprop kdb.input.device.disable` and confirm with **Enter**.  
 ⇒ 0 must be displayed.
  3. Plug the USB keyboard into the USB port.  
 ⇒ USB keyboard is activated.

## 9.9 Deactivating the USB keyboard with an SSH client

- ✓ USB keyboard is plugged in to the USB port.
- ✓ SSH client is connected to terminal.  
[Connecting the SSH client to the terminal \[► 9.7\]](#)
- 1. Enter the command `setprop kdb.input.device.disable 1` and confirm with **Enter**.
- 2. (Check setting.)  
Enter the command `getprop kdb.input.device.disable` and confirm with **Enter**.  
⇒ 1 must be displayed.
- 3. Unplug USB keyboard from the USB port.  
⇒ USB keyboard is deactivated.

## 9.10 Accessing terminal files with an SFTP client



### NOTICE

#### Deleting, moving and editing files

Incorrect actions lead to malfunctions or device failure.

- Use correct directories/files
- Before editing a file, make a backup copy.
- Observe the specified syntax for file contents.

- 
- ✓ **SFTP client** (e.g. WinSCP) is installed on the computer.
  - ✓ **SSH server** on the terminal is activated.  
[Activating or deactivating the SSH server \[► 9.6\]](#)
  - ✓ **SSH key file** is available.  
Default: kaba-private-ssh-key.ppk; if SSH key file has been changed, use the customer-specific SSH key file.
1. Start SFTP client.
  2. Set up connection.

Setting	Value
Transmission protocol	SFTP
Server address	<IPv4 address of the terminal>
Port	22
User name	root
password	kaba
SSH authentication → Private key	<Path to the file>

3. Click Log in.
  - ⇒ The Passphrase window is displayed.
4. Enter **passphrase** (**kaba** or customer-specific).
  - ⇒ Window with file directory computer/terminal is displayed.

## 9.11 Displaying the functional scope of the license

The functional scope of the terminal depends on options. Options are activated with a license key.

- ✓ [Accessing the service interface on the terminal \[▶ 6.5.1\]](#)  
[Accessing the service interface on the computer \[▶ 6.5.2\]](#)

1. Select **License** under System in the main menu.

⇒ The functional scope of the current license is displayed via the parameters.

Entry	Meaning
CardLinkEnabled=	CardLink function
EncryptionEnabled=	Data encryption via UDP and HTTPS
AccessControlEnabled=	Door control
LocalEnrollmentEnabled=	Capture of fingerprints at the terminal.
PartnerInterfaceEnabled=	Support for partner applications
NativeAppEnabled=	Launching of native apps via the device software (HR)
Browserenabled=	Browser access by the device software
MobileAccessEnabled=	Booking using a smartphone in conjunction with an MRD reader
AdditionalInputStepsEnabled=	Additional input steps during a booking process

### Other parameters

Entry	Meaning
ReplacementEnabled=true	Replacement device supplied by dormakaba This device must be put into operation using one-click replacement.

### License-based parameters

Entry	Meaning
ExpiryDate=	Validity date
Key=	License key
MAC=	MAC address
CreationDate=	Creation date

### Test license-based parameters

Entry	Meaning
TmpLicKeyCnt=	Shows how many more times a test license can be generated on this device.
TestLicenceEnabled=true	This license file is a temporary test license

## 9.12 Expanding the functional scope with a new license

The functional scope can be expanded by purchasing additional options. In this case, the existing license file must be replaced by the newly acquired license file.



### NOTICE

**The license file is invalid if the content is changed.**

An invalid license file will cause malfunctions.

- Do not change the contents of the license file.



### NOTICE

**The license file is invalid if it contains an incorrect MAC address.**

An invalid license file will cause malfunctions.

- Ensure that the MAC address matches.

- ✓ New license file (sop-ini) is available.
- ✓ [Accessing terminal files with an SFTP client \[▶ 9.10\]](#)
- 1. In the SFTP client, navigate to the license directory of the terminal.  
/data/data/com.kaba.apps.hr/files/init
- 2. Copy the new license file to the directory.
- 3. Restart the terminal.
- ⇒ The functions of the new license can be used.

## 9.13 Displaying system information

- ✓ [Accessing the service interface on the computer \[▶ 6.5.2\]](#)
- 1. Select **System information** under System in the main menu.
- ⇒ System information is displayed.

# 10 Packaging/Return

Assemblies and equipment which have not been packaged properly can incur costs due to damage during transport.

Please note the following information if dormakaba products are shipped.

dormakaba is not liable for damage to products due to insufficient packaging.

## 10.1 Complete Devices

The original packaging is specially adapted for the device. It offers the greatest possible protection against transport damage.



---

Always use the original packaging for returns.

---

If this is not possible, then ensure the packaging prevents damage to the device.

- Use a stable, thick-walled transport crate or a box. The transport crate should be large enough that there is 8–10 cm space between the device and the container wall.
- Wrap the device in suitable film or put in a bag.
- Pad generously around the device e.g. using foam padding or bubble wrap. It must be ensured that the device does not move within the packaging.
- Only use dust-free environmentally-friendly filling material.

## 10.2 Labelling

Including all returns paperwork and labelling the package correctly enables us to process your case quickly. Please ensure that a delivery note is enclosed in each package. The delivery note should contain the following information:

- Number of devices or components in each package.
- Article numbers, serial numbers, designations, order number.
- Address of your company/contact person.
- Reason for return, e.g. repair exchange.
- Accurate description of fault.

Returns from countries outside the EU also require a customs invoice with an accurate customs value and customs tariff number.

# 11 Disposal



The device is marked with the adjacent symbol indicating that disposal in domestic waste is prohibited.

The components of the device must be recycled or disposed of separately. Used devices contain valuable recyclable materials that need to be recycled. Toxic and hazardous components may cause permanent damage to the environment in the event of improper disposal.

At the end of their service life, the facility operator is obliged to return electrical and electronic equipment to the manufacturer, the point of sale or to public collection points set up for this purpose free of charge.

Disposal in Germany:

After termination of use, dormakaba EAD GmbH assumes the proper disposal of the delivered goods in accordance with the statutory regulations (ElektroG- Gesetz (electrical and electronics equipment law) in Germany). Any transport costs incurred to the manufacturer's plant are to be borne by the owner of the electrical equipment.

Disposal in Switzerland:

The appliance must be returned to an electrical device collection point in accordance with VREG (ordinance on recycling and disposal of electrical and electronic equipment).

In the EU, electrical appliances must be disposed of in accordance with country-specific waste disposal and environmental directives.

## Deletion of personal data

The erasure of personal data before disposal must be carried out self-dependent.



## Dispose of packaging in an environmentally-friendly manner.

The packaging materials are recyclable. Please do not put the packaging in with household waste, instead dispose of with waste for recycling.

# Index

<b>A</b>			
Ambient conditions		10	
Ambient temperature		10	
Android		9, 18, 54	
Android navigation buttons		44	
AoC		33	
Audio		9	
Automatic registration via B-COMM		41	
<b>B</b>			
Back		44	
BaseApp		18	
Bluetooth		9	
browser		38	
<b>C</b>			
cable cover		28	
Cable grommet		13	
Cable grommet plug		13	
Cable grommets		14	
CardLink		33	
CE label		13	
certificate		40	
Cleaning the housing		52	
CPU unit		9	
<b>D</b>			
Date of manufacture		13	
Delivery contents		13	
device software		7, 54	
DHCP server		31, 32	
Display		9	
Disposal		63	
DoC		33	
<b>F</b>			
Fingerprint reader		10	
firewall		31	
fixed IP address		32	
FTCS server		31	
<b>H</b>			
Home		44	
<b>I</b>			
Impact resistance		10	
IP address		38	
IT security		33, 40, 57	
<b>L</b>			
license		60, 61	
<b>M</b>			
MAC address		61	
Marking		13	
Memory		9	
Menu		44	
Mounting plate		13	
<b>N</b>			
Navigation bar		44	
Navigation buttons		44	
<b>O</b>			
Operating system options		9, 18 60, 61	
<b>P</b>			
Packaging		62	
PoE		9	
Protection class		10	
protection class IP65		14, 29	
<b>R</b>			
Reader		10	
registration mode		32	
Relative humidity		10	
Return		62	
RFID		9	
RFID reader		10	
<b>S</b>			
Search		44	
Serial number		13	
Service interface		18, 19, 38, 39, 40, 56, 60, 61	
service interface password		7, 19, 39	
SFTP client		18, 56, 59	
SFTP installer		54	
SSH client		18, 56, 57, 58	
SSH key file		7, 57, 59	
SSH server		7, 18, 31, 56, 57, 59	
Symbols		44	
System		9	
<b>T</b>			
tamper detection		15	
terminal password		7	



Test program 18  
Type plate 13

## U

USB keyboard 57  
USB port 57, 58

## W

web server 7, 18, 31, 38, 56  
WEEE Directive 63  
WLAN 9, 32





04500552 - 07/2024  
Copyright © dormakaba 2024



[www.dormakaba.com](http://www.dormakaba.com)

dormakaba Deutschland GmbH  
Albertstraße 3  
78056 Villingen-Schwenningen  
Germany  
T: +49 7720 603-0  
[www.dormakaba.com](http://www.dormakaba.com)  
Company headquarters: Ennepetal