BEYOND SECURITY   KABA®

B-eco

Manual

EN

1   About this manual

Validity This manual describes the Kaba **B-eco** terminal starting from

Manufacturing date:	February 2014
Serial number:	079940-000100
Service module version:	697-00-X-K07
B-Client PDC6 version:	766-01-X-K00
	767-01-X-K00

This manual describes all device versions and optional equipment and functions. Options must be purchased and are therefore only available if they were purchased. Additional equipment and functions may not yet be available at the time of issuing the manual and can possible only be purchased at a later stage.

Addressees This manual is written exclusively for specialists.

The descriptions in this manual are intended for personnel trained by the manufacturer. The information in this manual cannot substitute the product training.

The contents of this manual is intended for use by the following groups of people:

- **Project manager**

  Project manager who is responsible for the system and entrusted with project planning and realization.

- **Fitter**

  Person specialized in mounting and installation.

  Person who has an adequate technical training and sufficient experience and who has been authorized by the manufacturer after completing the training on the product.

- **Service technician**

  Specialist for initial set-up and maintenance of the installation.

  Person who has an adequate technical training and sufficient experience and who has been authorized by the manufacturer after completing the training on the product.

- **Network administrator**

  Realizes the set-up of the device within the network and makes sure that the devices are accessible within the network.

- **Software partner**

  Specialists for connecting the system to the user software by defining operating and booking sequences, programming the customer applications and setting the parameters of the devices.

Important!

For reasons of device safety, some of the activities might only be carried out by the SERVICE PERSON.

Only persons of the groups "Fitter" and "Service technician" have the status of a SERVICE PERSON according to DIN EN 60950-1:2006.

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

Additional documentation   Terminal software:

- B-Client PDC6 software manual, order number 04043881.

Service functions and FTP access:

- BECO Service Module manual, order number 04106694.

Orientation in the manual   This manual contains the following orientation aids to facilitate finding of specific topics:

- The table of contents at the beginning of the manual gives an overview of all topics.
- The header always contains the respective main chapter.
- An index in the alphabetical order is given at the end of the manual.

Danger categories   Remarks with specifications or rules and restrictions to prevent injuries and property damage are particularly marked.

Please read the danger warnings and user tips carefully. This information will help prevent accidents and damage to your equipment.

Danger warnings are divided into the following categories.

CAUTION

Describes a possibly dangerous situation that can lead to minor injuries.

NOTICE!

Important information for proper handling of the product.

Ignoring this information can cause device malfunction and the device or something near it can get damaged.

Symbols   Depending on the source of danger, warnings are marked with symbols of the following meaning.

	General danger		Danger for electronic components due to electrostatic discharge

Remarks   Please pay special attention to the remarks that are marked with symbols.

Tips and useful information.

This information will help you to best use the product and its functionality.

2   Grouped safety messages

The device has been built in accordance with state-of-the-art standards and the recognized safety rules. Nevertheless, its use may constitute a risk to persons and cause damage to material property.

Read and observe the following safety instructions, before using the product.

2.1   Use as directed

The device or system is only intended for usage as described in chapter "Product description."

Any use beyond the designated use is not according to rules. The manufacturer is not responsible for damages resulting from improper use. The user/operator is responsible for any risks associated with non-duly use.

2.2   Mounting and Installation

Mounting and installation may only be carried out by the SERVICE PERSON (see chapter 1 / Addressees).

Installation may only be carried out in places that fulfill climatic and technical conditions stated by the manufacturer.

Kaba GmbH is not liable for damages resulting from improper handling or incorrect installation.

2.3   Service and Maintenance

Maintenance work / troubleshooting

Only the SERVICE PERSON (see chapter 1 / Addressees) is entitled to remove faults and carry out the maintenance work.

Reconstruction and modification

Any reconstruction and modification of the device may only be realized by the SERVICE PERSON (see chapter 1 / Addressees). All reconstructions and modifications carried out by unauthorized personnel shall render void any liability.

2.4   Handling lithium batteries

The device has a lithium manganese dioxide battery, type CR2032, to buffer the memory. The battery is on the rear of the terminal housing.

> **CAUTION**
>
> Lithium batteries can rupture or burst like an explosive.
>
> Improper handling of lithium batteries can cause fire and explosions.
>
> •   Lithium batteries may only be replaced by the SERVICE PERSON.
>
> •   They may only be replaced by batteries of the same type.
>
> •   Do not open, bore through, or crush lithium batteries.
>
> •   Do not burn lithium batteries or expose them to high temperatures.
>
> •   Do not short-circuit lithium batteries.
>
> •   Do not recharge the lithium batteries.

2.5   ESD (electrostatic discharge) protective measures

> **NOTICE!**
>
> Danger for electronic components due to electrostatic discharge.
>
> Improper handling of printed circuit boards or components can cause damages that lead to complete failures or sporadic errors.
>
> •   During installation and repair of the device, the ESD protective measures must be considered.

The following rules must be considered:

•   Wear an ESD wristband when handling electronic components.

       Connect the end of the wristband to a discharge socket or an unvarnished grounded metal component. This way, static charges are discharged from your body securely and effectively.

•   Touch only the edges of circuit boards. Do not touch the circuit board nor the connector.

•   Place all dismantled components on an antistatic surface or in an antistatic container.

•   Avoid contact between circuit boards and clothing. The wristband only protects the printed circuit boards against electrostatic discharge from your body, but there is still a risk of damage through electrostatic discharge from your clothing.

•   Transport and dispatch dismantled modules only in electrostatically shielded protective bags.

2.6   Environmental protection

Please do not dispose of the device in your domestic waste.

Used devices contain valuable materials that should be recycled. Properly dispose of used devices.

Used-up batteries must be disposed of according to state and local regulations.

Please store the batteries to be disposed of carefully in order to avoid short-circuits, crushing, or damage to the battery housing.

3   Product description

3.1   B-eco
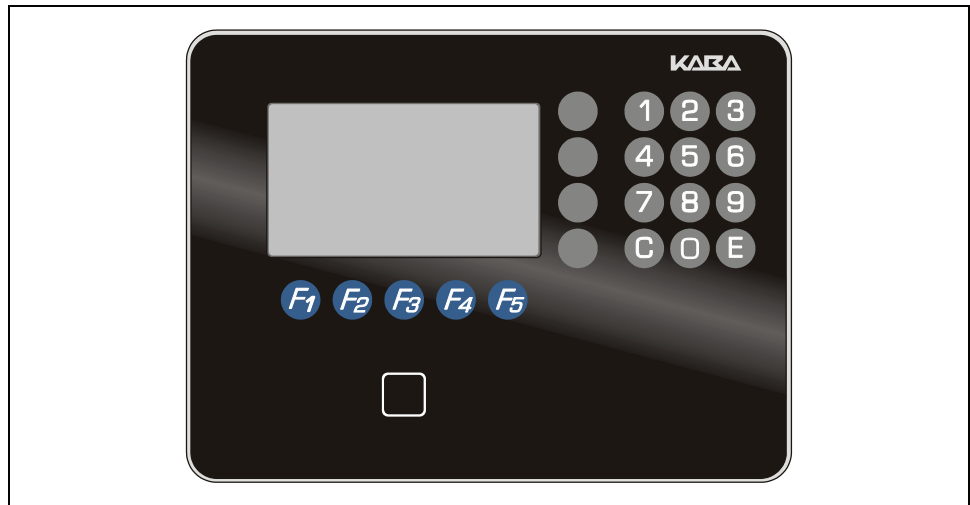
The terminal has been designed for shop floor data collection (SFDC) functions and can also perform time and attendance functions or can be used for project time recording.

The B-Client PDC6 terminal software is used on the terminal. Data records of the B-Net and B-web terminal series are compatible with the data records used in this device.

The terminal software can be updated any time via a software update.

In combination with the B-COMM communication software, the device offers a new and comfortable concept for start-up, subsequent functional upgrades and device analysis.

To display time data and information, the terminal has a graphic monochrome display with a resolution of 240 x 128 pixels.

The device has capacitive key fields that are operated by touching the glass front. The function keys are designed for time and attendance and SFDC.

Time data are entered via a contactless RFID reader, a biometric reader or a swipe card reader, depending on the version.

An external reader (e.g. CCD scanner) can optionally be connected.

Communication is established via the Ethernet network and power supply via PoE (Power over Ethernet).

Optionally, the terminal has 1 output (relay) and 2 digital inputs for control functions.

3.2   Technical data

3.2.1   System

Kaba BECO330 CPU unit with ARM7TDMI processor core

Memory

•   8 MByte Flash

•   16 MByte SDRAM.

•   2 MByte SRAM, buffered

Modified parameters, master records, and data records are retained approximately 6 months without power supply.

Graphic monochrome display

•   240 x 128 pixels resolution.

•   Background illumination by white LED.

Capacitive keypad

SFDC version:

•   5 function keys (F1 to F5).

•   4 special keys (grey).

•   Numeric keypad with C and E keys.

XML version:

•   5 function keys (F1 to F5).

•   8 special keys (gray).

•   Alphanumeric keypad (multiple assignment) with C and E keys.

3.2.2   Inputs / Outputs

1 relay output (optional)

•   One potential-free changeover contact.

•   Contact rating: 30 V AC / DC; max. 2 A

Only voltages from limited power sources according to EN 60950-1 may be applied.

2 digital inputs (optional)

•   Controllable against GND via dry contact.

•   Controllable via external direct voltage, switching level:

    –   Active input: 0 V to 0.8 V

    –   Inactive input: 2.5 V to 24 V

3.2.3   Interface

Ethernet interface

•   IEEE802.3 compatible 10BASE-T/100BASE-TX Auto sensing, Auto MDIX.

3.2.4   Reader

Supported RFID technologies (depending on design):

•   LEGIC prime/advant

•   MIFARE Classic/DESFire

•   HID iCLASS

•   HID Prox

Biometric reader (optional add on reader)

•   Compact Biometric Module (CBM) with integrated database for fingerprints. Depending on the version, the reader has a storage capacity of 500, 3000 or 5000 persons (2 fingers per person).

        The reader is available in 2 versions:

        –   CBM

        –   CBM-E with enhanced approvals (PIV-IQS with FBI certification and FIPS 201-approved template evaluation)

•   Supported authentication methods:

        –   Biometric identification

Swipe card reader (optional add on reader)

•   Magnetic stripe track 1, 2, 3

•   Barcode redlight

•   Barcode infrared

RJ45 connection for external reader

•   Interface: RS-232C.

•   Communication parameters: 9600, 8, N, 1.

•   Power supply for the reader: 5 V DC, max. 300 mA over RJ45 connection.

3.2.5   Power supply

PoE (Power over Ethernet)

Power supply of the terminal via the 8-wire Ethernet cable (max. 100 m).

- Corresponds to IEEE 802.3 af

- Power consumption class 3, max. power consumption 12.95 W

- Supported powering processes:

    - Spare pair powering
      over (Fast Ethernet free) wire pairs 4/5 and 7/8

    - Phantom powering
      over RX wires (1/2) and TX wires (3/6)
      Power supply is superimposed to the data signal

3.2.6   Uninterruptible power supply (option)

The optional uninterruptible power supply (UPS) guarantees operation for up to 15 minutes or approx. 200 bookings in case of power failure. Whatever occurs first.

Requirement: New battery, 90% charged, temperature 20 - 25 °C.

The battery is completely charged after 10 hours.

3.2.7   Environmental conditions

- Ingress protection according to IEC 60529:

    - IP30

    - IP54 (Option for devices with RFID reader)

- Relative humidity:

    - 5% to 95%, non-condensing

- Environmental temperature:

    - 0 °C – +40 °C (operation)

    - -25 °C – +70 °C (storage)

3.2.8   Dimensions

Terminal housing and mounting plate

All dimensions in mm.
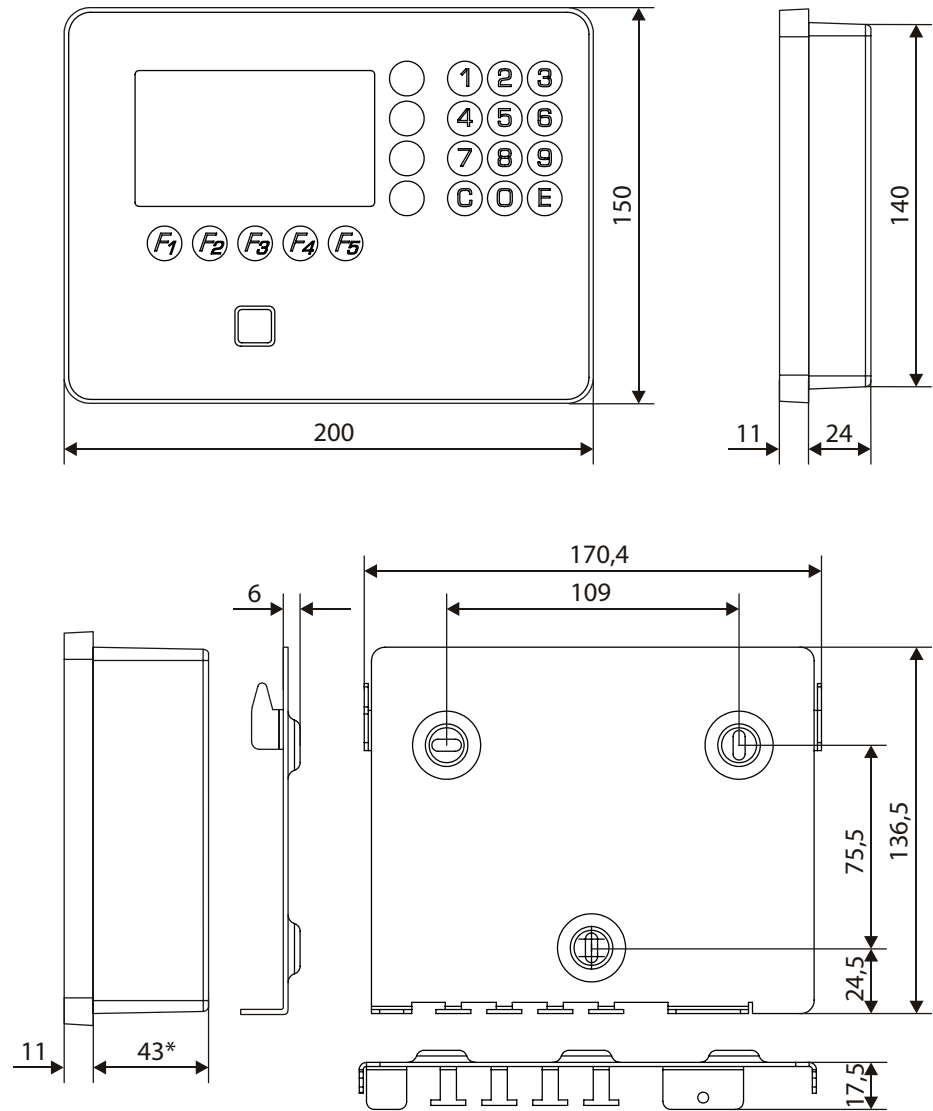
* Deep housing for unit with optional UPS

Terminal housing with biometric reader and mounting plate
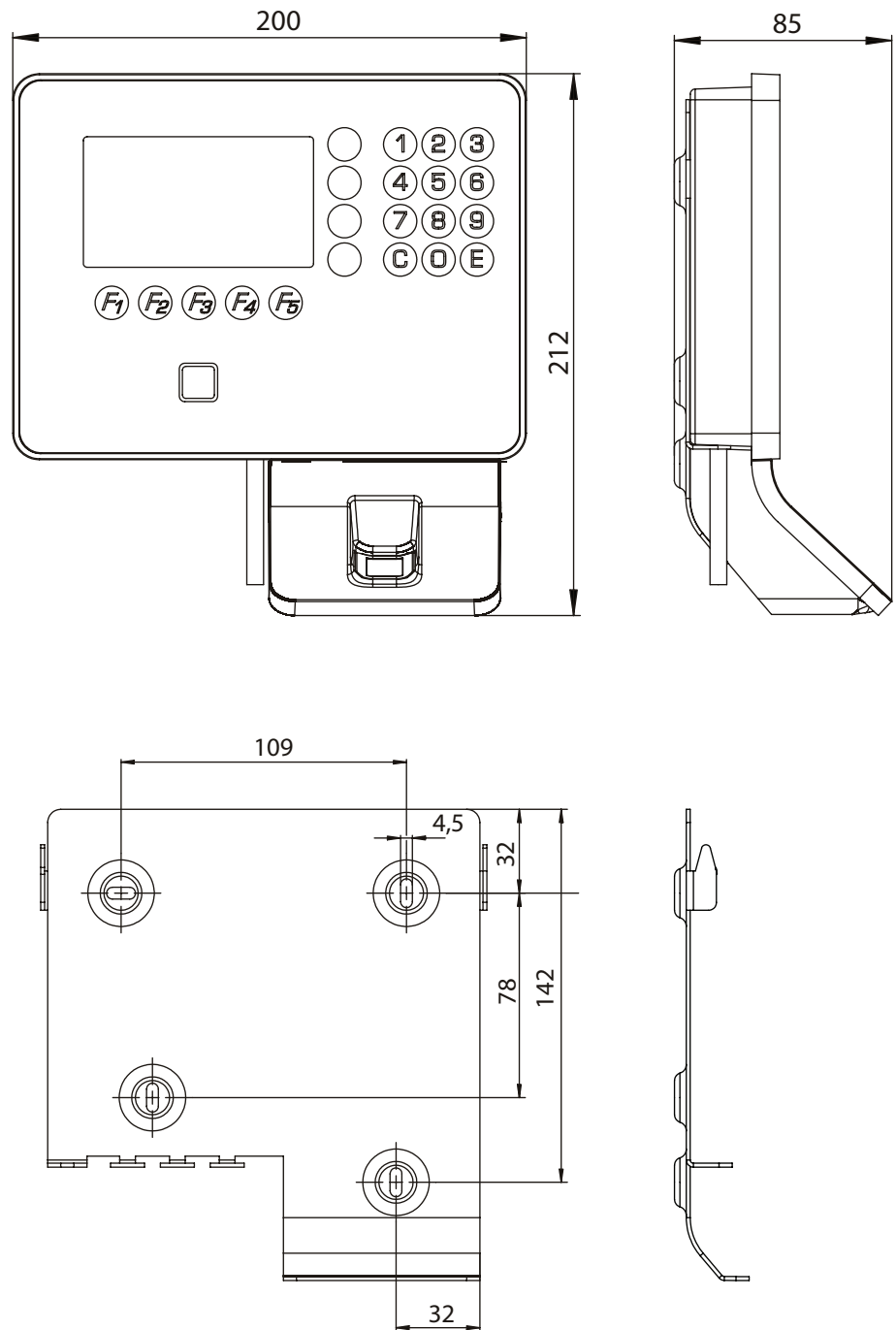
Terminal housing with swipe card reader and mounting plate
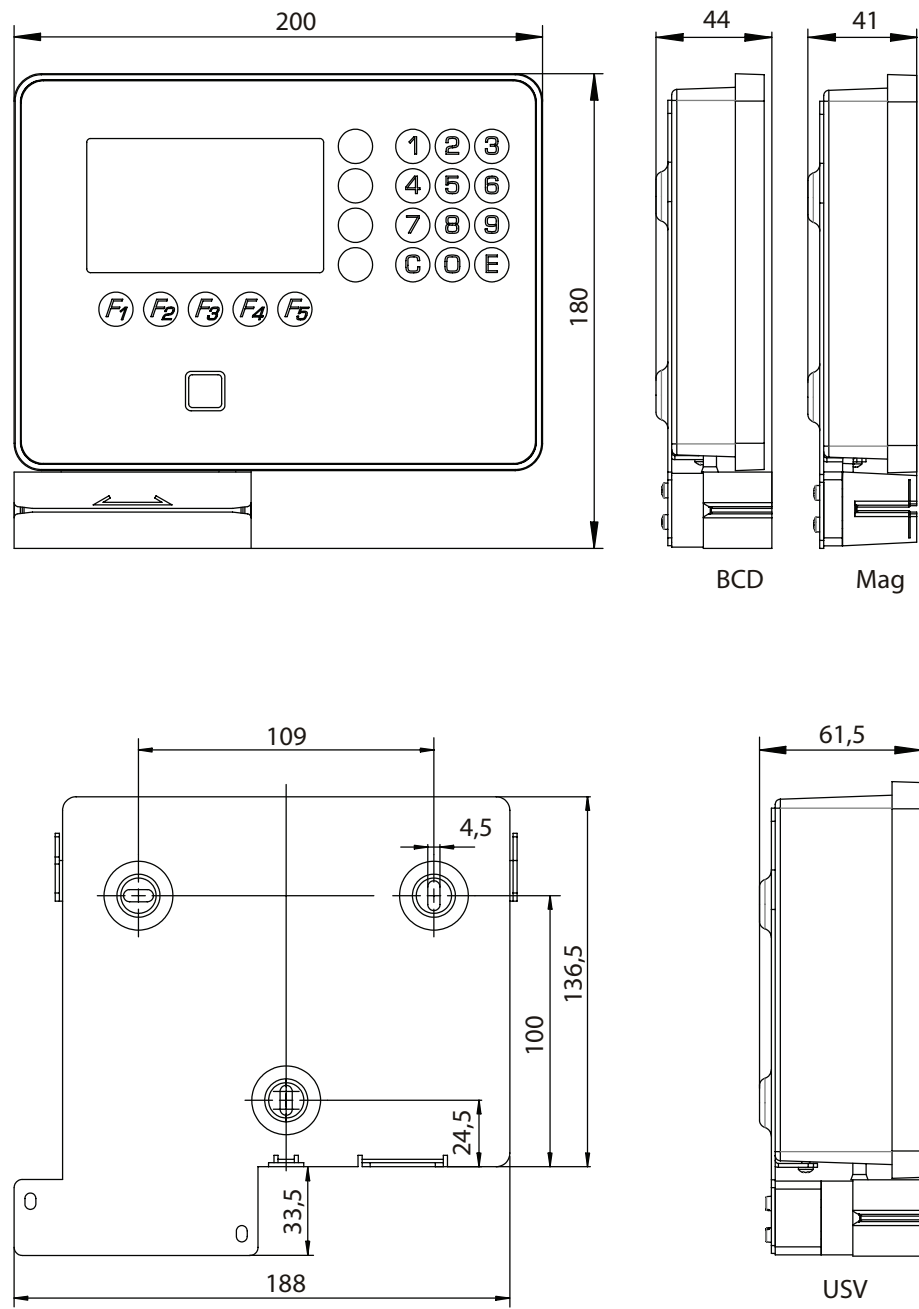
3.3   Conformity

This device complies with the following standards:

EN 60950-1/A12:2011

EN 300 330-1 V1.7.1

EN 300 330-2 V1.5.1

EN 301 489-1 V1.4.3

EN 301 489-3 V1.9.2

according to the regulations of the EU Directives

1999/5/EC   R&TTE Directive

DECLARATION OF CONFORMITY

according to FCC Part 15

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference

- This device must accept any interference received, including interference that may cause undesired operation.

Please Note:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Device variants

- B-eco with LEGIC   FCC ID: NVI-B-ECOL1

- B-eco with MIFARE   FCC ID: NVI-B-ECOM1

- B-eco with HID Prox   FCC ID: NVI-B-ECOH1

- B-eco with HID iCLASS   FCC ID: NVI-B-ECOH2

3.4   Labeling

The identification plate is located on the bottom side of the device.
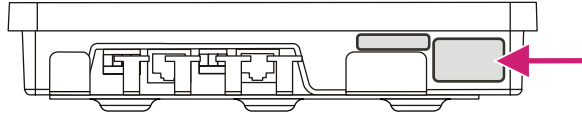
Specified on the identification plate:

- Device name
- Product number
- Serial number
- Power data
- CE identification
- FCC identification
- WEEE labeling acc. to DIN EN 50419

4   Design and Function

4.1   Device structure
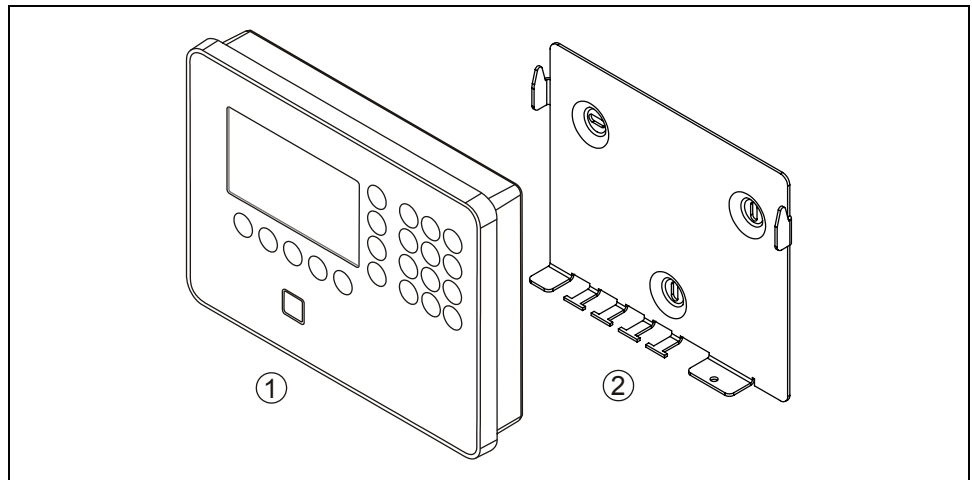
The device consists of the terminal housing (1) and the mounting plate (2).

The mounting plate is the wall-mounting element of the device. The terminal housing is simply snapped into the mounting plate and secured by means of a screw from below.

The installation lines are led into the device from below. The connections are located on the rear of the terminal.
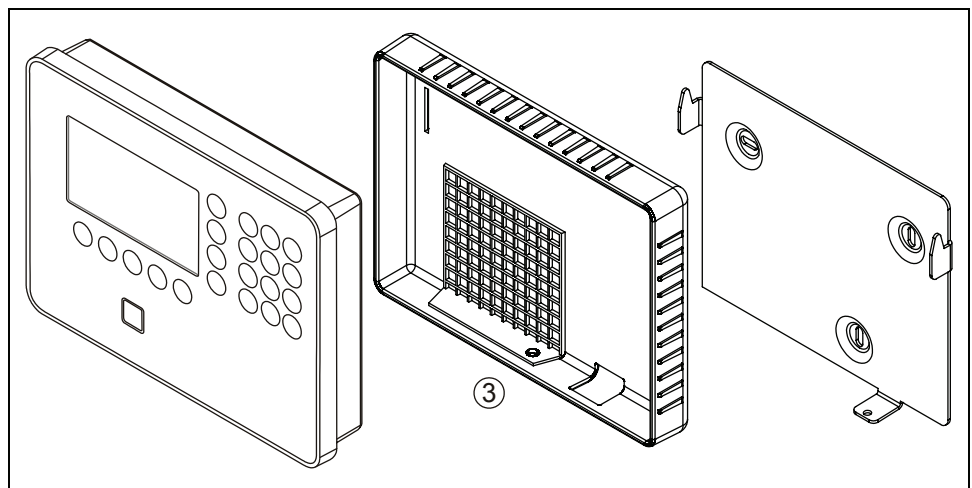
RFID devices with optional IP54 ingress protection are equipped by an additional sealing (3).

4.1.1   Terminal front
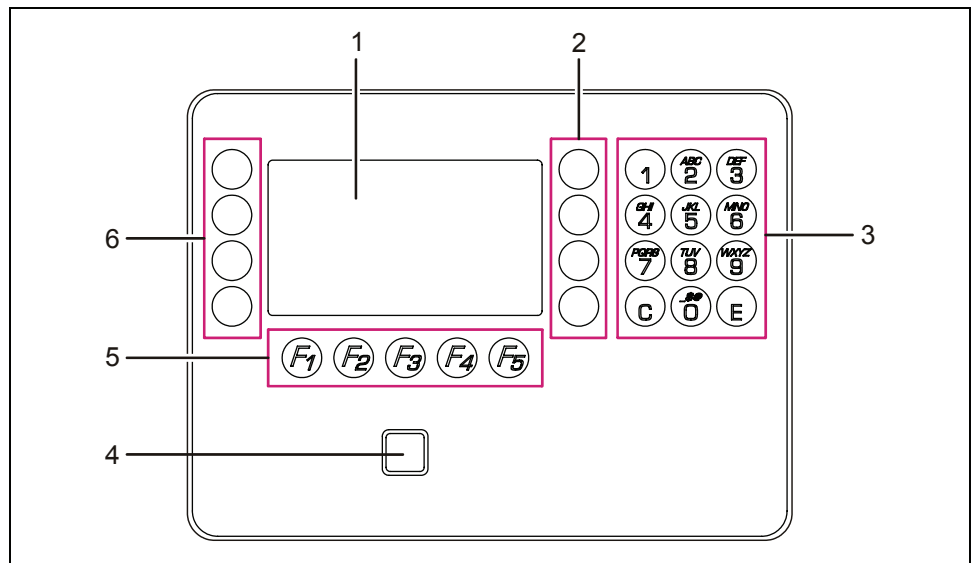
1   Display

2   Special keys S01 to S04

3   Numeric keypad for SFDC version,
        alphanumeric keypad (with multiple assignment) for XML version

4   RFID reader

5   Function keys F01 to F05

6   Special keys S05 to S08 (only with XML version)

4.1.2   Terminal rear
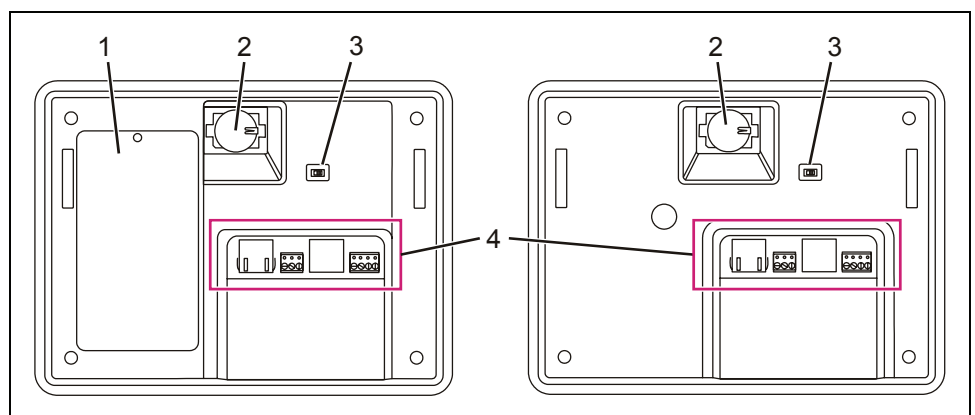
Device with UPS   Device without UPS

1   UPS cover (only devices with UPS)

2   Buffer battery

3   Service switch

4   Device connections

4.2   System connection

4.2.1   Communication principle

Communication between the terminal and a higher-level host computer usually takes place via an Ethernet network.
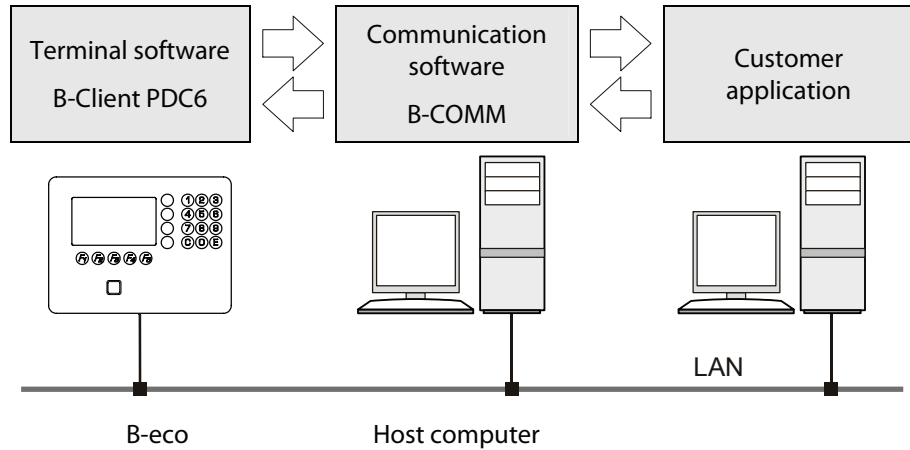
Data exchange between the B-Client PDC6 terminal software and the customer application takes place by means of the B-COMM communication software.

The communication software transfers the data recorded by the terminals to files or sends it to the customer application via a defined interface.

4.2.2   Parameterization

The various terminal functions mainly depend on the set parameters. Parameter setting allows extensive adaptation to a wide range of applications. A parameter setting changes the currently valid parameters and stores the new ones in the memory of the terminal. The required parameters are provided by the customer application and transferred to the terminal in form of parameter records.

4.2.3   User rights

Information required for authorizations is provided by the customer application in the form of personnel master records.

All the information on a specific badge number or group is stored in the master record. The master record contains information on authorizations, time profiles, person-related display texts and the PIN number.

Master records can be saved in the terminal. This allows the terminal itself to decide whether a booking is authorized. Master records can be transmitted to the terminal at any time. The currently valid master record is then overwritten. Individual master records can be deleted from the host. Likewise, master records can be requested from the host. The number of master records that can be loaded in the terminal depends on the licensed memory configuration.

Whether a booking is authorized can also be requested by contacting the host in "online" mode. In this case, no master records are required in the terminal.

4.2.4   Terminal data

After a booking has been made, a data record is generated by the terminal. The data record contains information about who has booked on which terminal using which function key.

The operating mode of the terminal determines when this data record is transmitted to the host.

As a result of certain statuses and events, alarm records and status records will be generated.

4.2.5   Operating modes

4.2.5.1 Online

After a booking has been made, the terminal carries out the checks and writes the test result as error identification into the input record. The data record is transmitted to the host computer. After that, the terminal expects a logical booking response from the host. With this response the terminal is informed by the host if the booking is authorized or not.

If the terminal does not receive a logical booking response from the host, it will change to the offline operating mode and decide itself if the booking is authorized or not. As soon as the host is available again, all data records stored offline since the last transmission are transmitted to the host. Then the terminal changes back to the online operating mode.

4.2.5.2 Offline

After a booking has been made, the terminal carries out the programmed checks and decides immediately by way of an internal booking response if the booking is authorized or not. Otherwise, the data records will be stored in the terminal. As soon as the host computer is available, all data records stored since the last transmission are transmitted to the host.

4.2.5.3 Autonomous

After a booking has been made, the terminal carries out the programmed checks and decides immediately by way of an internal booking response if the booking is authorized or not. Data records of authorized or unauthorized bookings are stored in the terminal, depending on the set parameters.

If the host is available, any existing error and alarm records are transmitted to the host.

The stored data records are transmitted to the host in a special data record after being requested.

4.3   Device variants and options

4.3.1   Hardware variants

4.3.1.1 Keypad

The terminal is available with 2 different keypads.
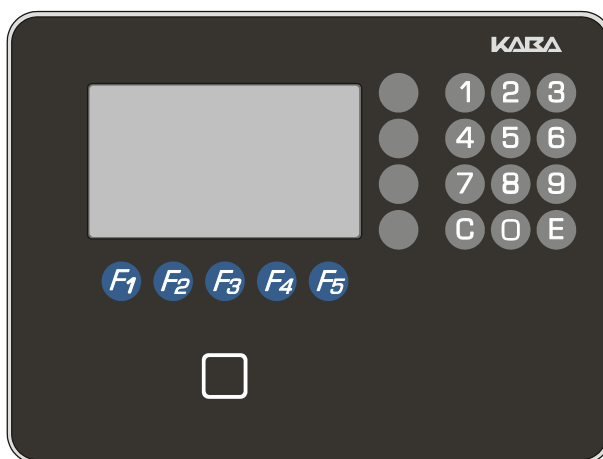
- • SFDC keypad
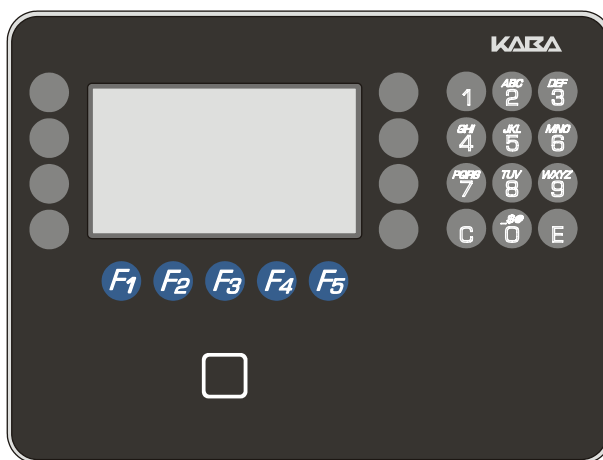
- • XML-keypad

4.3.1.2   Reader

RFID reader

The terminal can be equipped with different RFID readers
(see chapter 3.2.4).

The RFID reader is integrated in the terminal housing.

Biometric reader

Optional the terminal can be equipped with a biometric reader
(see chapter 3.2.4).
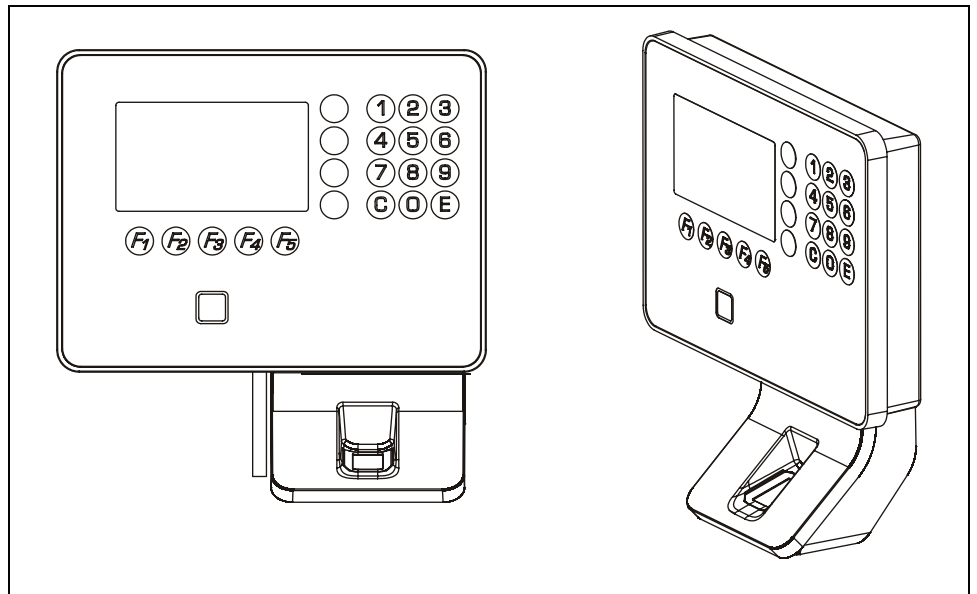
The biometric reader is integrated in an add-on housing.

Swipe card reader

Optional the terminal can be equipped with a swipe card reader for magnetic stripes
or bar codes (see chapter 3.2.4).
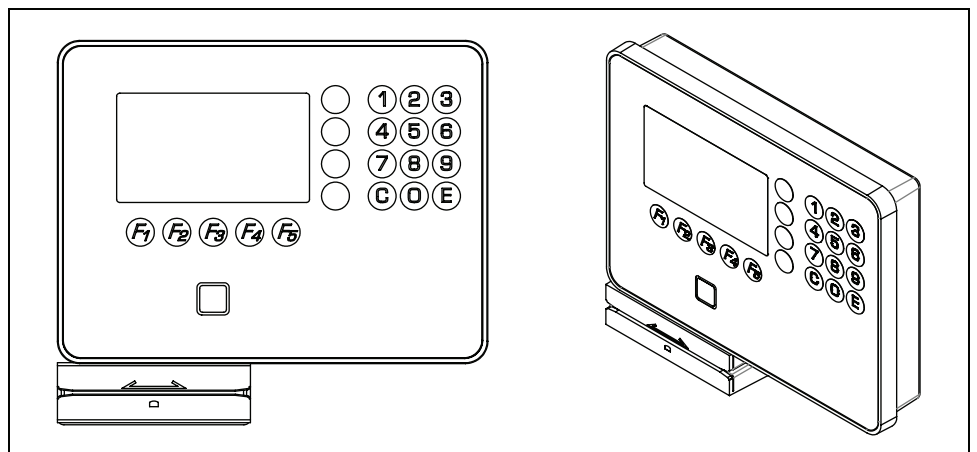
The swipe card reader is designed as a bottom-mounted reader.

4.3.1.3   Ingress protection

As an option the device is available with IP54 ingress protection. In this case the device is equipped b y an additional sealing. This option is only available for devices with RFID reader, not for devices with add-on readers.

4.3.1.4   UPS

The device is optionally equipped with an uninterruptible power supply.

The UPS guarantees operation when power supply fails temporarily. Devices with integrated UPS have a deeper terminal housing.

4.4   Terminal software

The B-Client PDC6 terminal software is used on the device.

The B-Client PDC6 terminal software performs the following basic functionalities:

- •   Host communication via
    - –   UDP
    - –   http/https
- •   Operating mode
    - –   online
    - –   offline
    - –   autonom
- •   Display info and mailbox texts
- •   G dialog
- •   List report
- •   200 master records, 4,000 data records

4.4.1   Terminal software variants

B-Client PDC6 is available in the following two variants.

Partner Client (767-0x-X-K0x)

Not usable with B-COMM ERP.

ERP Client (766-0x-X-K0x)

Usable with B-COMM ERP.

> **i**   Generally the B-Client PDC6 terminal software version 766 is installed on the device. The terminal software version 767 depends on the available functions of the software license.

4.4.2   Software options

The usable functionality of the device is based on the options purchased by the customer. The individual options are activated by means of a license key in the "sop.ini" license file.

4.4.2.1   Memory options

	Standard	Option 1	Option 2*		Option 3
Master records	200	1000	2000	3500	5000
Data records	4000	4000	8000	3000	20000

*The selection of the 2000/8000 or 3500/3000 variant is made by entry in the b-client_pdc6.ini file.

4.4.2.2   Data encryption

Requirement:

•   Only together with the B-COMM communication software.

Allows:

•   Data encryption via Ethernet UDP.

         The user data is encrypted with a key length of 448 bits via the Blowfish algorithm. The key is exchanged automatically via the Diffie-Hellman algorithm.

•   Data encryption via HTTPS.

4.4.2.3   Inputs / Outputs

Allows:

•   Use of 2 digital inputs.

•   Use of 1 relay output.

4.4.2.4   Local enrollment

Requirement:

•   Devices with biometric reader CBM.

Allows:

•   Recording of new fingerprints over CBM reader in the terminal.

4.4.3   License file

The **sop.ini** file is stored in the **/Program/Share/Init/** directory.

This file contains the license key for the basic software and software options purchased by the customer. The license key is bound to the MAC address of the device.

> The contents of the sop.ini file may not be modified. Any manual change will invalidate the license.

The parameters allow you to see which functions are enabled.

Entry (example)	Meaning
[BClientPDC6]	Section of B-Client PDC6 terminal software
BufferConfiguration=2	Memory options 0 to 3
	The following parameters each have the value true or false.
BClientPDC6Enabled=true	B-Client PDC6 terminal software
ERPClientEnabled=true	true = useable with B-COMM ERP false = not useable with B-COMM ERP
DigitalIOEnabled=true	true = Inputs / Outputs available false = Inputs / Outputs not available
EncryptionEnabled=true	true = Encryption available false = Encryption not available

5   Installation

5.1   Installation conditions

5.1.1   General

An accurate installation of all components is a basic requirement for a properly functioning device. The following installation instructions must be adhered to.

5.1.2   Installation site

Clearances

Keep a distance of 20 cm on all sides between two devices with RFID readers.

Mounting height

The recommended mounting height is 140 cm to the top edge of the terminal.

Electromagnetic fields

The terminal must not be installed in the area of strong electromagnetic fields caused by switching power supply, power lines, phase controllers, etc.!

Electromagnetic fields can affect the reading power or cause failures, in particular with contactless readers (RFID).

Sun exposure

Direct sun exposure leads to reflections within the display area and a poor readability of the display.

Please avoid installation at places with direct sunlight.

5.1.3   Connections

The following connectors must be prearranged at the installation site of the terminal.

- Ethernet network connection

  Established via the network cable are

  – Communication with the host computer

  – Power supply for the terminal via PoE (Power over Ethernet)

- Signal lines to inputs/outputs (optional).

Ethernet network connection

The shield of the network cable must be connected to ground at the destination side.

PoE (Power over Ethernet) power supply

PoE (Power over Ethernet) facilitates the power supply of the terminal via the 8-wire Ethernet cable (max. 100 m). This avoids a separate power supply cable to the terminal. Power is supplied to the device after plugging in the Ethernet cable (for details, see chapter 3.2.5).

Power is ideally supplied to the terminal over a PoE power injector (PoE switch or midspan PoE injector) integrated into the IT rack to the network cable.

5.1.4   Cable entry
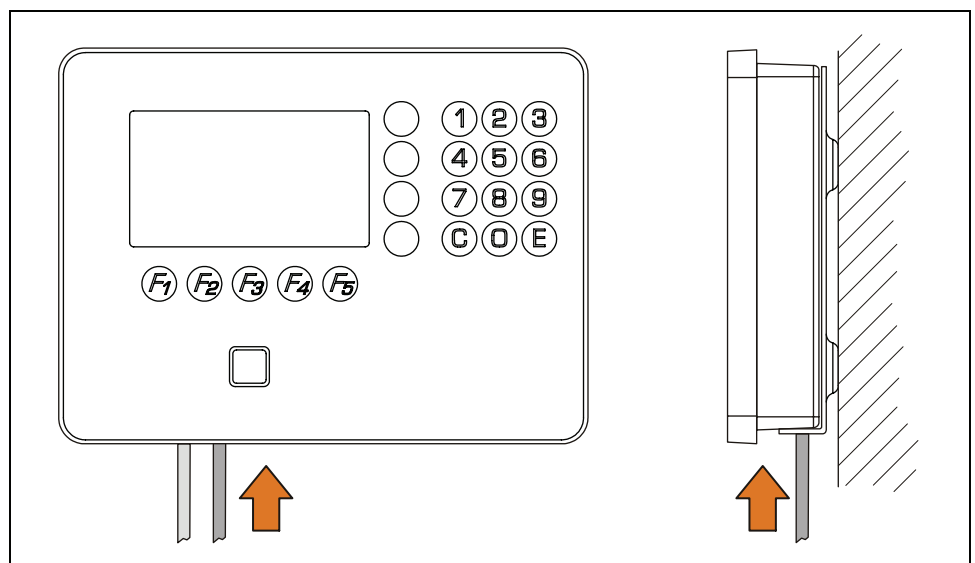
The installation lines are led into the device from the bottom.

5.2   Installation lines

5.2.1   Ethernet

Network cable with RJ45 connector, line requirement CAT.5 E or higher.

5.2.2   Inputs - Outputs

The terminals for the signal lines are designed for the following max. wire sizes:

Diameter: 0.3-1.4 mm

Cross section: 0.08-1 mm^2

AWG number: 28 - 16

Recommended cable:

CAT.5 S-UTP 4 x 2 AWG 24 or AWG 22 (according to EIA/TIA568) or higher.

5.3   Attach mounting plate
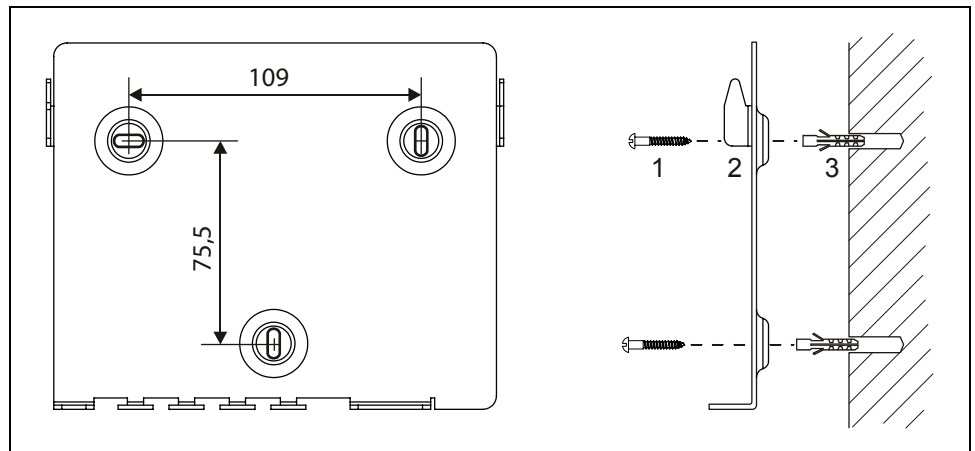
Fastening the mounting plate, dimensions in mm

The mounting plate (2) is mounted directly to the wall using screws (1) / dowels (3). There are three oval fastening holes for fastening the mounting plate.

Fixing material (included in the delivery):

•   3 round-head wooden screws DIN 96 Ø 4.5 x 35 (1)

•   3 dowels S6 (3)

When mounted on different surfaces, use suitable fastening material.

In case of soft mounting surfaces, make sure that the housing is not pressed into the surface when mounting it.

The unevenness of the mounting surface may not exceed 0.5 mm. Use washers, for example, to compensate a possible unevenness.

Mounting dimensions mounting plate for devises with biometric reader
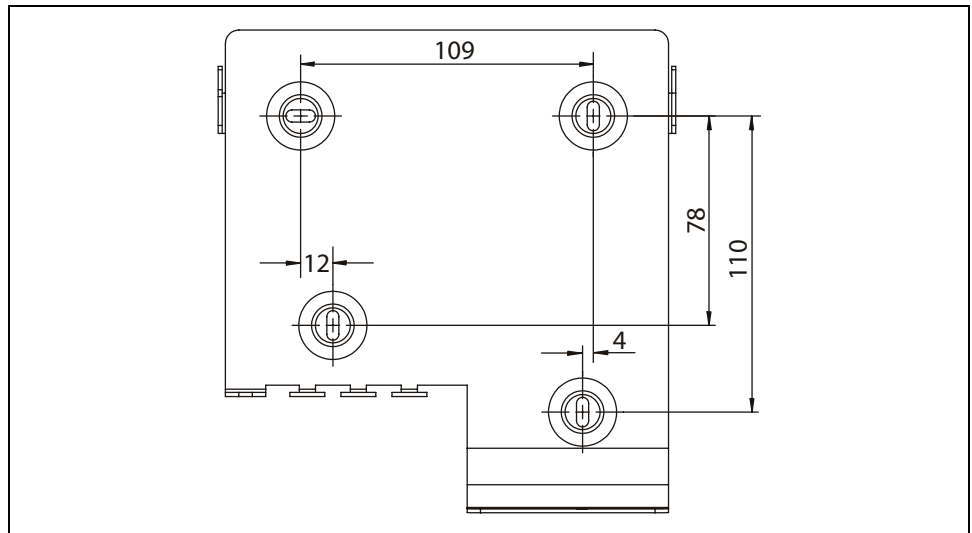
Mounting dimensions mounting plate for devises with swipe card reader
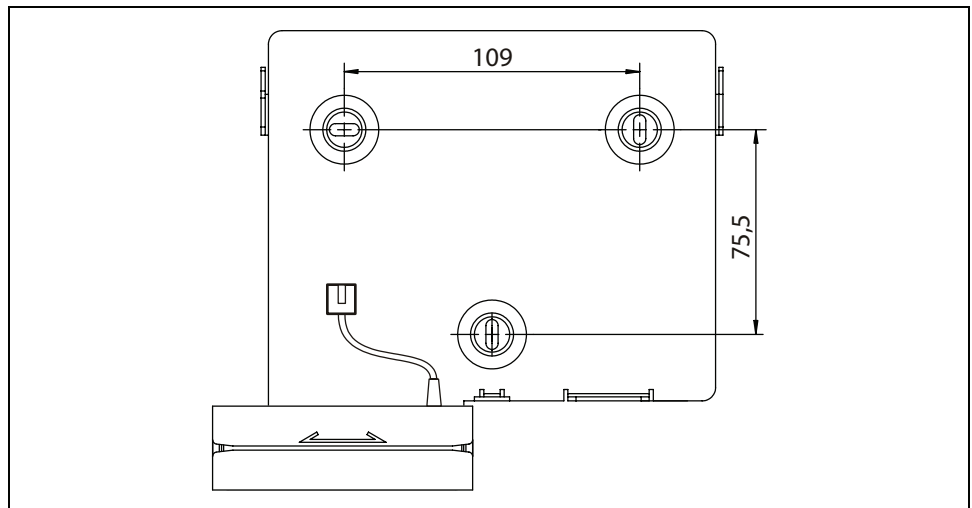
5.4   Inserting batteries

Only devices with UPS!

Before commissioning the device, the batteries for the uninterruptible power supply (UPS) must be inserted.

A blister pack containing 6 batteries is included in the delivery of the device.

Specification: NiMH battery, 1.2 V, capacity min. 2000 mAh, size AA

NOTICE

Wrong battery types or incorrectly inserted batteries can overheat and damage the device.

·   Use new identical batteries conforming to the above specification only.

·   Do not use any primary battery cells.

·   Ensure correct polarity.

·   Remove the TORX8 screw (arrow).

·   Remove the cover of the battery compartment.

·   Press batteries into the holding clamps.
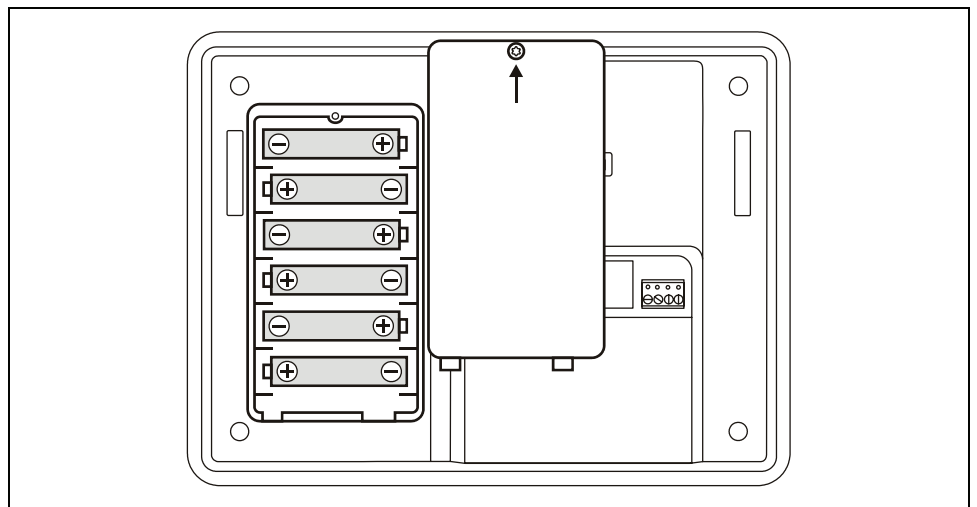
·   Re-attach cover.

After an operating time of about 10 hours, the batteries are completely charged, and the UPS is ready for use.

5.5   Connections
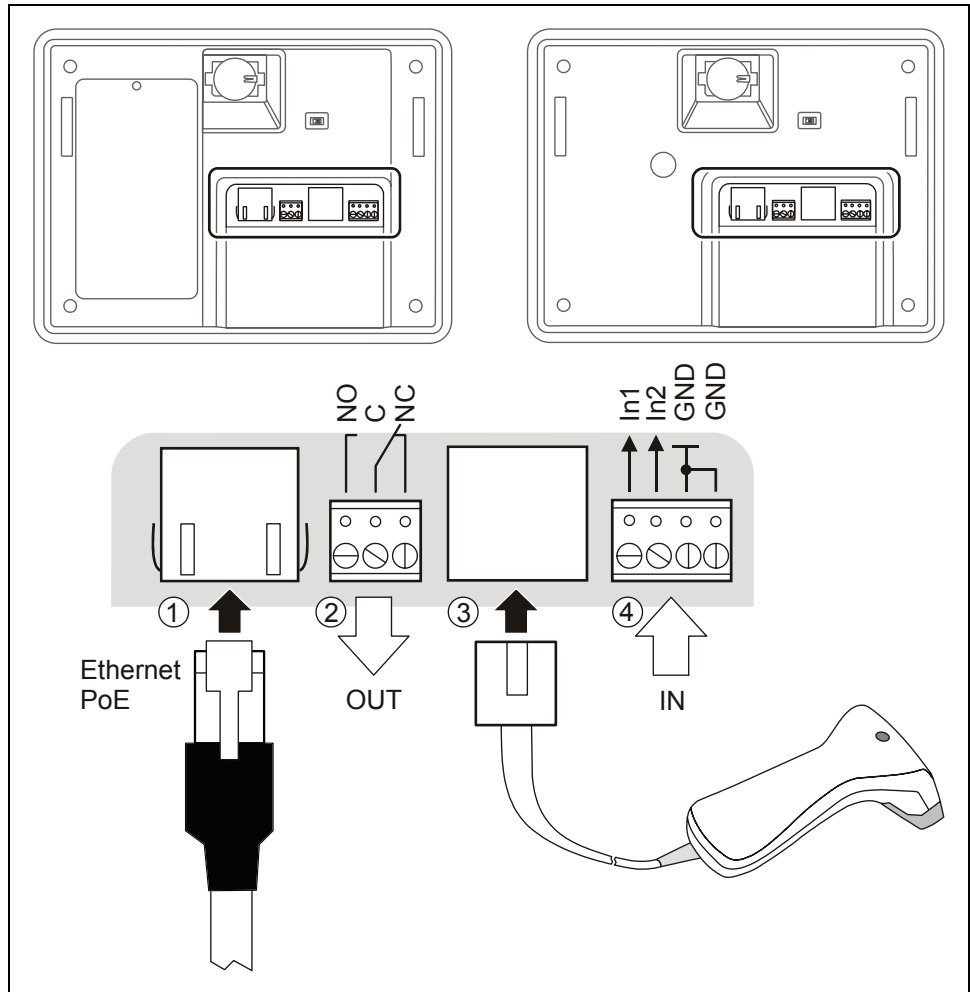
1   RJ45 Ethernet network connection

        Communication with the host and power supply of the terminal via PoE

2   Terminal block for the relay output

        Max. contact rating 30 V AC / DC; 2 A

        Only voltages from limited power sources according to EN 60950-1 may be
        applied.

        The relay can be used to trigger the door opener. For door openers, which are
        supplied with direct current, a freewheeling diode must be connected in
        parallel to suppress interference (in reverse direction). A varistor must be
        connected in parallel to AC door openers.

3   RJ45 connection for an external reader or the optional swipe card reader

4   Digital inputs

        The inputs are connected to common ground using a simple switch or relay
        contact.

5.5.1   Connecting an external reader

The swipe card reader is connected to this socket at devices with optional swipe card reader.

An additional external reader with RS-232C levels, e.g. a CCD barcode scanner, can be connected to the device.

The reader is connected to the COM1 port of the device.

The reader must be configured and enabled via the service module so that it works properly.

Assignment of the RJ45 socket (3)

	Pin 1	5 V DC; max. 300 mA	Pin 5	TxD (of the reader)
	2	CTS*	6	GND
	3	GND	7	RTS*
	4	RxD (of the reader)*	8	5 V DC

* Not supported, do not use connection!

Hardware handshake is not supported, no transmission delay for scanner data, communication parameters: 9600, 8, N, 1 (can be set).

Power supply for the reader

The power supply of the external reader is effected via the 5 V DC of the RJ45 socket. The permitted current is max. 300 mA.

5.6   Fastening the terminal housing to the mounting plate
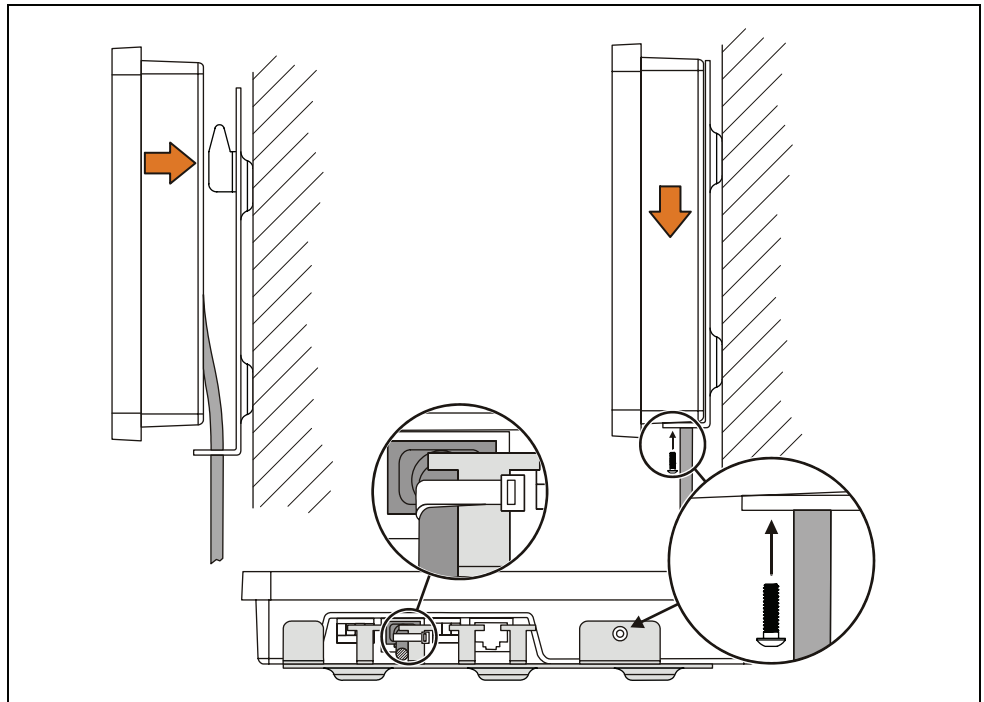
Fasten the terminal housing to the mounting plate as follows:

1   Hang terminal housing into the mounting lugs of the mounting plate and slide it downwards.

2.   Secure terminal housing on the mounting plate using locking screw K30x10 TORX.

3.   Strain-relieve the installation lines on the mounting plate using cable binders.

5.7   Fastening of devices with additional sealing (IP54 version)

Fasten the terminal housing to the mounting plate as follows:

1.   Insert the installation cables through the cable inlets on the bottom of the sealing and connect them to the device.
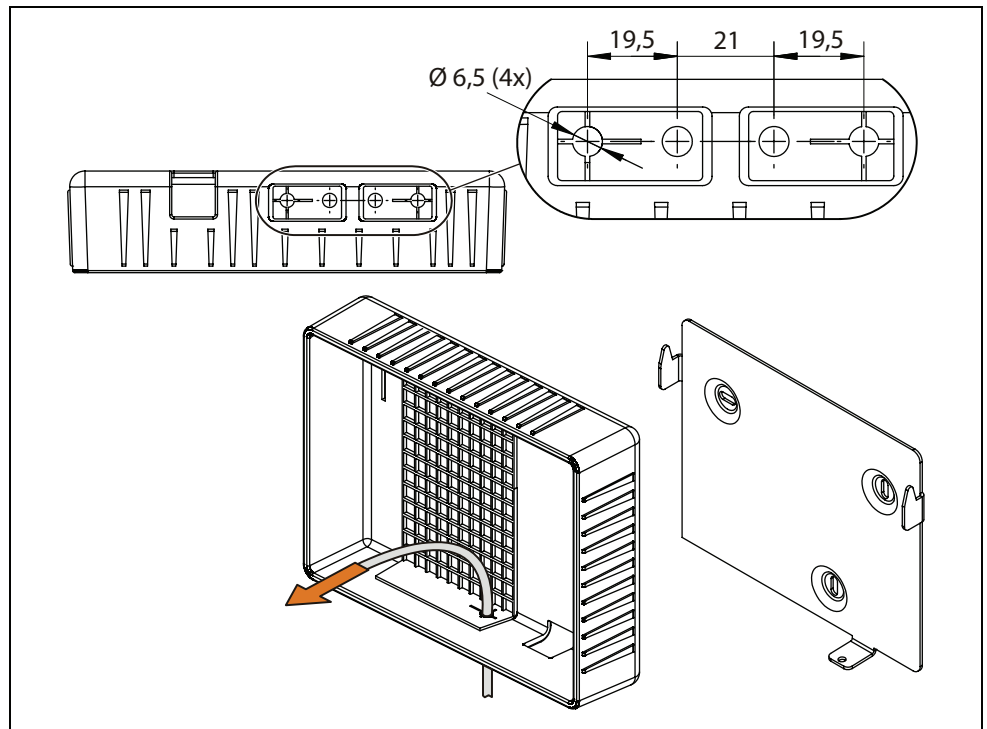
2.   Slide sealing through the terminal housing from behind.

3.   Hang terminal housing into the mounting lugs of the mounting plate and slide it downwards.

4.   Secure terminal housing on the mounting plate using locking screw K30x10 TORX.
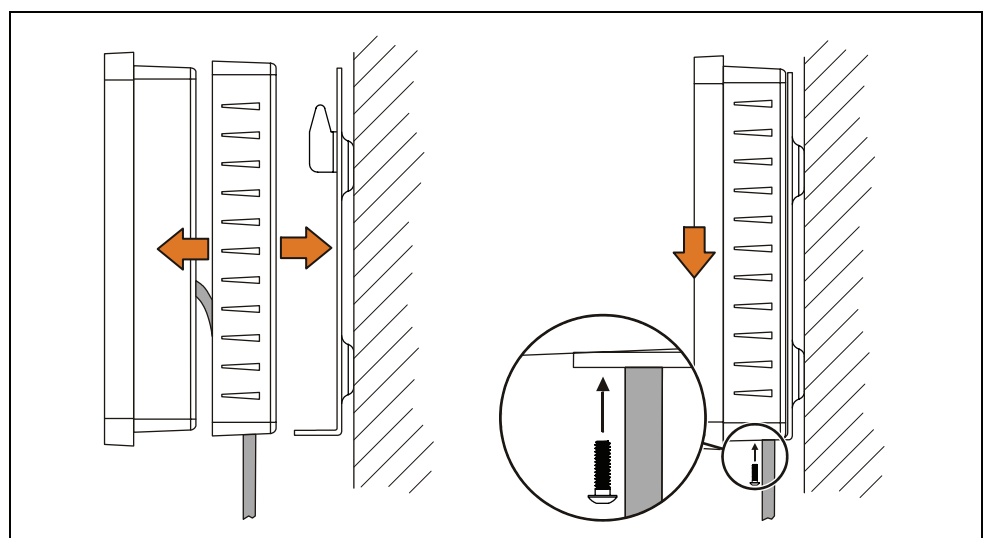
6   Start-up

6.1.1   Service switch

There is a service switch on the rear of the terminal housing. The service switch is accessible after having removed the terminal housing from the mounting plate.
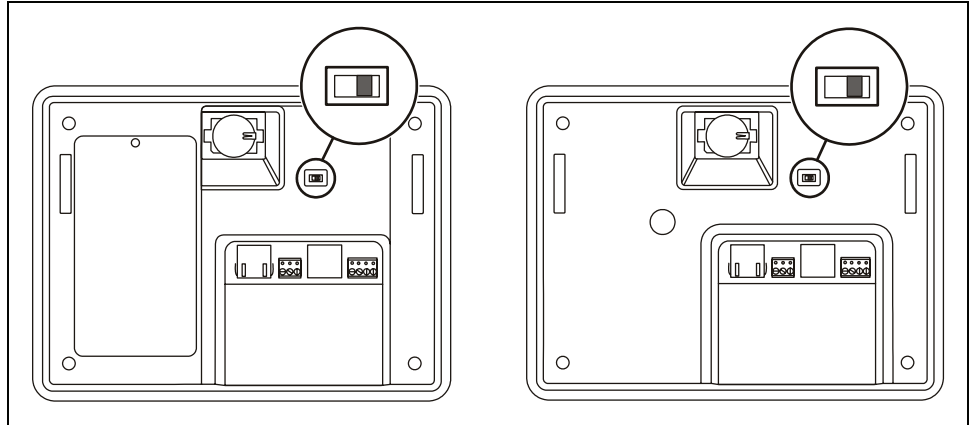
The terminal software recognizes when connecting it whether the switch has been modified. Then press a numeric key on the device front to start one of the functions described in the following.

If you do not press any key within 30 seconds, the device starts with the terminal software.

Procedure and possible functions

*   Remove the device from the mounting plate.

*   Switch off the power supply (unplug network cable).

*   Change the position of the slide switch.

*   Switch on the power supply (plug in network cable).

         Two short acoustic signals sound, darkening the display.

*   Press a key (numeric keypad on housing front)

    –   Key "**1**" = Cold start

    –   Key "**3**" = Start of the service mode

    –   Key "**7**" = Start of the service mode and setting of the service IP

         A short acoustic signal sounds, brightening the display.

6.1.2 Cold start

The data memory is deleted and newly initialized with a cold start of the system. A cold start becomes necessary, for instance, after a software update or after having changed the memory configuration. The device starts with the terminal software.

When performing a cold start, parameters are reset to their default values. Master records and booking records are deleted.

Network settings as well as group and terminal addresses remain unchanged.

In devices with active "host registration", the B-COMM Java communication software transmits automatically all previously valid parameters after a cold start.

6.1.3 Starting the service mode

If the device is started in service mode, then the service module is loaded alternatively to the terminal software.

The service module provides the functions that are required for setup, maintenance, and diagnosis of the device.

6.1.4 Starting the service mode and setting the service IP address

This start option allows the service mode to be started and simultaneously the terminal IP address to be set to 123.0.0.2 and the network mask to 0.0.0.0.

Any already set IP address is overwritten. DHCP is deactivated.

All other settings, such as host IP address, UPD port number and GID/DID, remain unchanged.

6.1.5 Starting the terminal software / warm start

The device starts the terminal software when it does not recognize any changed switching status when it is connected (normal system start).

How to perform a warm start:

·   Switch off the power supply (unplug network cable).

·   Switch on the power supply again (plug in network cable).

6.2   Network access requirements

An Ethernet network is used for startup and maintenance of the terminal as well as communication in production use.

To guarantee unhindered and trouble-free data traffic, the UDP ports used for communication must be free.

Modify the firewall configuration accordingly.

6.2.1   Communication

The UDP port used for communication between B-COMM and the terminal must be free.

The UDP port is located in the range of 7700 hex to 77EF hex (30464 dez. to 30703 dez.) depending on the configuration.

If communication is established via http/https, the port used must be free (normally port 80 or 8080).

6.2.2   Comparing finger templates

Devices with a biometric CBM reader require another UDP port for exchanging biometric data.

The UDP port used for the FTCS or BCFTC stream must be free.

The UDP port is located in the range of 7800 hex to 78EF hex (30720 dez. to 30959 dez.) depending on the configuration.

6.2.3   1-click installation

It must be possible to transfer UDP data packages unhindered to the B-COMM server.

- IP address 239.255.255.250, UDP port 1900 dez. and UDP port 7900 (30976 dez.) must be free.

- The SSDP service has to be enabled in the Windows service management.

- The FTP connection over standard port 21 must be free.

6.2.4   Configuration

The terminal is configured by means of the service module. Standard port 80 is used for access with an http browser.

Standard port 21 is used for the FTP connection to the terminal.

6.3   1-click installation

In combination with the B-COMM communication software, the terminal can be put into operation almost automatically.

System requirements

•   B-COMM communication software version 3.7 and higher.

Required settings (activated by default when delivered)

•   Network configuration via DHCP.

•   DNS configuration via DHCP.

•   Check box "Enable host registration" ticked.

The device is preset in the factory for 1-click installation.

6.3.1   Start-up procedure

•   Plug in network cable and supply device with power.

•   After booting, the device cyclically reports to the B-COMMs active in the network.

At this point, the following display is shown until start-up by a B-COMM is complete:

```
                  B-eco
Serial number:          <Serial
number>
IP address:              <IP address>


      Waiting for registration
```

•   After the device is found by B-COMM, the relevant data that identify the device are queried.

•   If the device is not known, it is entered in B-COMM under the *B-COMM Terminal Discovery* client under the *BCTDS (Terminal Discovery Stream)* stream.

•   If the device is to be managed using B-COMM, it can be moved to the desired stream, and the communication parameters can be set.

•   After having assigned the device firmly to B-COMM, B-COMM first updates the settings of the device and then makes a backup copy together with the "sop.ini" license file.

•   After loading the specific parameters and master records from the host, the device is automatically restarted and is then ready for operation.

•   The device now informs the B-COMMs active in the network that registration is complete. Other B-COMMs then remove the device again from the *BCTDS* stream.

6.4   Manual settings

Device settings can also be made manually. This might be required, for example, to define a fixed network address or to configure later hardware extensions.

There are the following options to adapt the parameters:

- **Service mode**

  For the setting of the parameters via menu-controlled service functions per HTTP browser, see BECO service module manual.

- **Remote setup**

  Modify the parameters via FTP (see BECO service module manual).

- **B-COMM**

  Modify the parameters via the "Terminal basis settings" menu item (see BECO service module manual).

6.5   Configuration-specific settings

In the following, we present the required settings for various device configurations.

The settings can be made using service functions in the menus of the service mode, see BECO service module manual.

It is also possible to transfer the parameters in the **reboot.cmd** file via FTP to the device, see BECO service module manual.

The following parameter examples correspond to the entries in this file.

6.5.1   Ethernet settings

These settings are required if the terminal is integrated into an Ethernet network. For details, please see the BECO service module manual.

6.5.1.1   Assigning fixed terminal network parameters

```
[Ethernet]
DHCP Mode=disabled
Terminal Addr=10.10.5.85
Netmask=255.255.0.0
Gateway Addr=10.10.1.101


DNS Configuration from DHCP=disabled
DNS Addr=0.0.0.0
```

6.5.1.2   Assigning terminal network parameters via DHCP

```
[Ethernet]
DHCP Mode=enabled


DNS Configuration from DHCP=disabled
DNS Addr=0.0.0.0
```

6.5.1.3   Requesting DNS settings via DHCP

```
[Ethernet]
DHCP Mode=enabled


DNS Configuration from DHCP= enabled
```

6.5.2 Host interface

6.5.2.1 Host communication via Ethernet / UDP

> ℹ️ Prefix hexadecimal parameter values with "**0x**" ,
> example UDP port=**0x7705**

```
[HostLine]
Host Line=ETH
Host Type=UDP
Host Addr=10.10.12.52
UDP Port=0x7705
Encryption=disabled
Host Registration=disabled
Group ID=01
Device ID=01
```

6.5.2.2 Host communication via Ethernet / XML (http/https)

```
[HostLine]
Host Line=ETH
Host Type=XML
Encryption=disabled
Online IP:Port=10.10.10.107:80
Proxy IP:Port=10.10.10.145:1234
Use Proxy Server=1
Group ID=01
Device ID=00
```

6.5.3 Reader settings

Example:

- Internal LEGIC reader to COM2
- External barcode scanner to COM1 (RJ45 socket)

```
[Reader1]
Interface=COM2
Type=LEGIC


[Reader2]
Interface=COM1
Type=BARCODE
```

6.6   Setting the screen contrast

The display contrast can be set by simultaneously pressing keys **C, 4, 9** (in this order).

First you are asked for the password. By default, no password has been set, which is why you should confirm by pressing "**E**".

The contrast is changed using the keys on the right from the display.

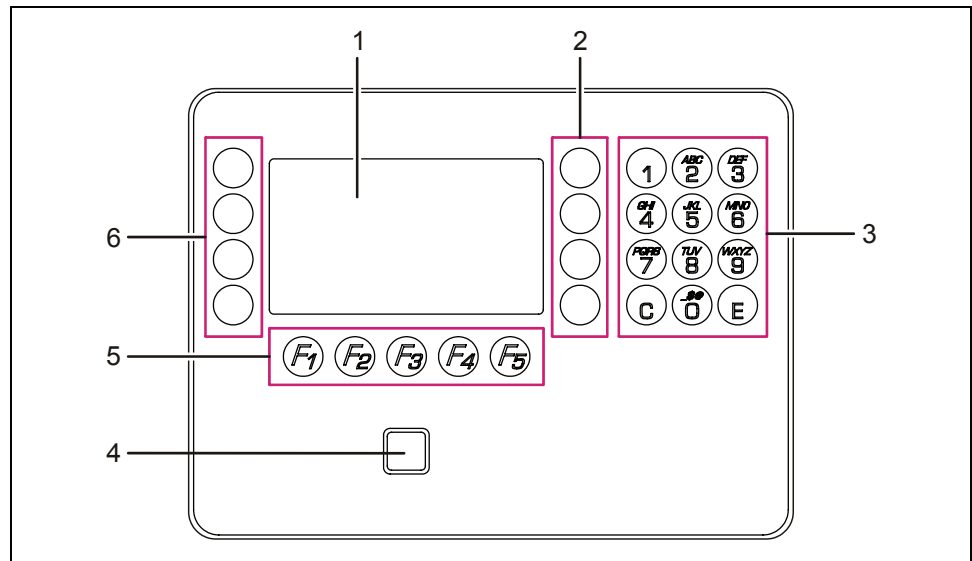|	
▲ (double) ○	Increase contrast, in steps of 5
255 ▲ ○	Increase contrast, in steps of 1
▼ ○	Reduce contrast, in steps of 1
▼ (double) ○	Reduce contrast, in steps of 5

Left from the symbols, the current numeric value for the contrast in the range from 230 to 290 is displayed. Default is 260.

Press key "**E**" to apply the value and exit the contrast setting.

7   Operation

7.1   Operating elements

| 1	Display
2	Special keys S01 to S04 (from top to bottom)
3	Numeric keypad for SFDC version, alphanumeric keypad (with multiple assignment) for XML version
4	Entry field of the RFID reader
5	Function keys F01 to F05
6	Special keys S05 to S08 (only with XML version)

7.2   Keypad

The individual keys of the keypad are capacitive keys.

Slightly press a key with your fingertip to operate the device.

Pressing a key is confirmed by an acoustic signal.

7.3   RFID reader

Hold contactless media simply in front of the entry field of the RFID reader on the terminal.
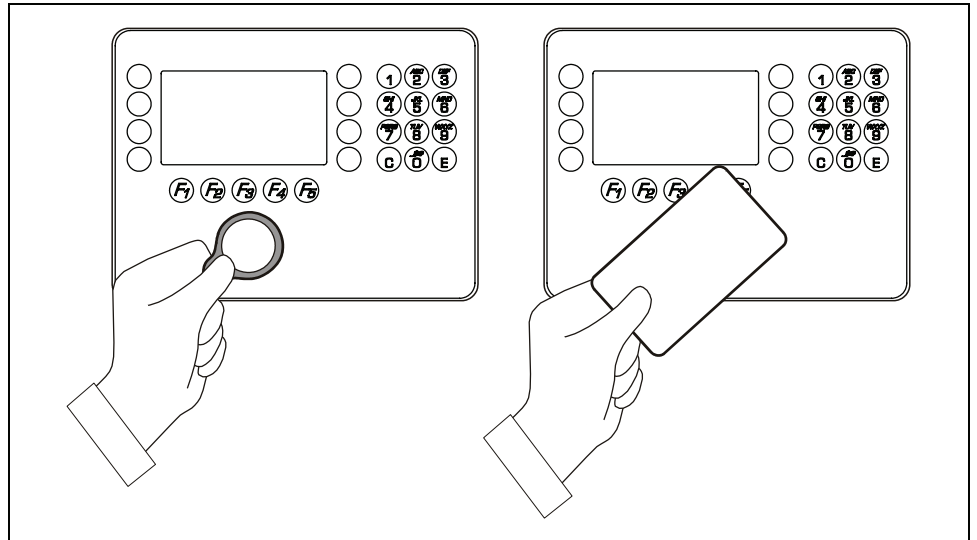
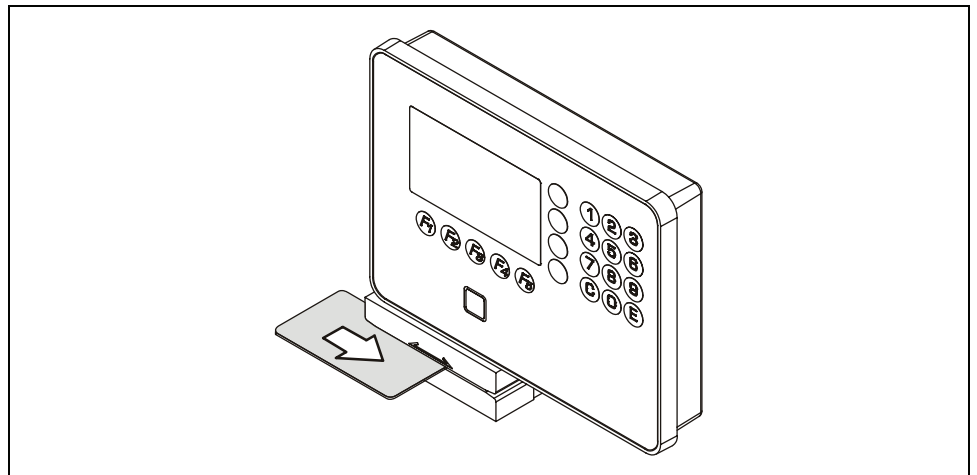After a valid booking, a short acoustic signal can be heard.

7.4   Swipe reader

Swiftly slide the magnetic-stripe badges and barcode badges through the reading bar in any direction.

The magnetic stripe is on the back of the badge, pointing toward the scanning unit.

The barcode is on the front of the badge, pointing toward the scanning unit.

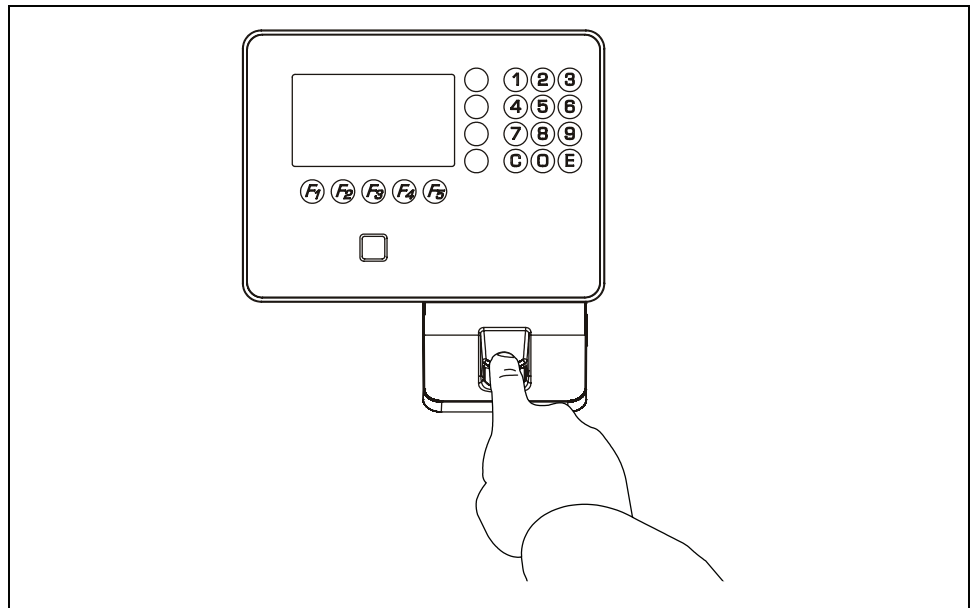After a valid booking, a short acoustic signal can be heard.

7.4.1 Biometric reader

In its basic state, the biometric reader is inactive.

1. To enable the reader, press a function key which directly requires a biometric entry.

   The reading window of the biometric reader is lit.

2. Place finger on the biometric reader sensor.

After a valid booking, a short acoustic signal can be heard.

7.4.2 Finger position

Only if finger position and pressure on the reader window are ideal, is a correct fingerprint read-in ensured.

Ideal finger position

• The finger has to be slightly humid.

• The finger has to be pressed gently onto the window.

• The fingerprint has to be in the center of the reader window.

7.4.3   Operator guidance

While the fingerprint is read in, the user is guided event-driven by the biometric reader.
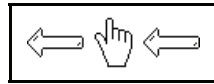
  Place finger more to the left.

  Place finger more to the right.

  Place finger more to the top.

  Place finger more to the bottom.

  Press finger stronger.

  Fingerprint already recorded in this position (latent finger) Place finger in other position again.

7.4.4   Displaying error states

The following symbols are displayed to signal the error states to the user.

  No finger templates available in the reader.
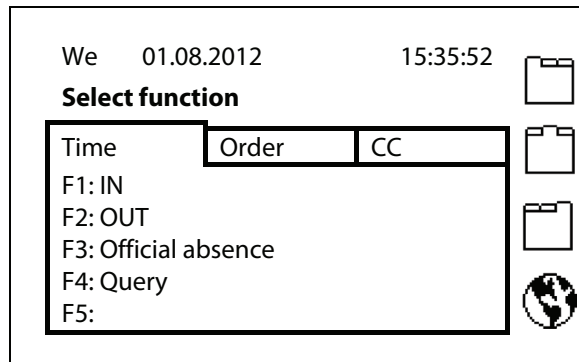
  Unknown fingerprint.

7.5   Operating sequences

The terminal functions and operating sequences depend on the set parameters. Parameter setting allows extensive adaptation to a wide range of applications.

The following examples refer to the B-Client PDC6 terminal software in its default setting.

7.5.1   Basic state

```
We     01.08.2012              15:35:52
Select function

Time            Order         CC
F1: IN
F2: OUT
F3: Official absence
F4: Query
F5:
```

In its basic state, the display shows tabs. A tab is selected by pressing special keys S1 to S3. The tab contains the currently correct assignment of the function keys.

Special key S4 is used to select the language.

7.5.2   Active function

```
We     01.08.2012              15:36:27
                   IN

              Present badge

F1: IN
F2: OUT
F3: Official absence
F4: Query
F5:
```
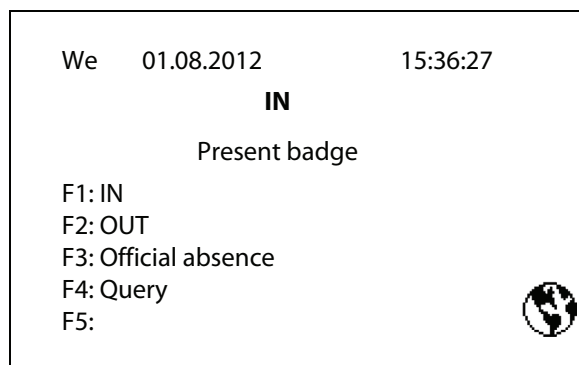
After selecting a function, you are asked for the first input step, for example "Present badge".

The valid assignment of the function keys for the current tab is still displayed even when the function has been activated. A different function can still be selected.

7.5.3   Active booking

```
┌─────────────────────────────────────┐
│                                      │
│   We    01.08.2012        15:36:40   │
│                  IN                  │
│              Please wait             │
│                                      │
│                                      │
│                                      │
│                                      │
└─────────────────────────────────────┘
```

After the first input step, the function key information is hidden.

7.5.4   Booking response

```
┌─────────────────────────────────────┐
│                                      │
│   We    01.08.2012        15:36:42   │
│                  IN                  │
│              Thank you               │
│                                      │
│                                      │
│                                      │
│                                      │
└─────────────────────────────────────┘
```

Once the booking response, for example "Thank you", has been displayed, the booking is complete.

7.6   Keypad entries

7.6.1   Numeric input

```
We      01.08.2012          15:56:11    -

              Beginning of order
              Machine number                  .

            ┌──────────────────┐
            │ 123|-----        │             ,
            └──────────────────┘

```

The input field is displayed by entering the first digit.

The digits are entered on the numeric keypad.

In addition, the characters minus, period and comma can be entered via the right-hand special key bar.

7.6.2   Alphanumeric input

```
We      01.08.2012          15:58:29    -

              Beginning of order
              Order number                    .

            ┌──────────────────┐
            │ 123ab|---        │             ,
            └──────────────────┘

                                            123
```

The alphanumeric input is done via the numeric keypad. The individual keys have multiple assignments.

In addition, the characters minus, period and comma can be entered via the special keys 1 to 3.

Special key 4 is used to switch the input mode:

•   **123** = Input of digits

•   **abc** = Input of small letters

•   **ABC** = Input of capitals

At the beginning of the input, the digit input is active, after the first press, it changes to the small letters input mode and then to the capitals input mode.

7.7   Local enrollment

It is possible to enroll fingerprints directly on terminals of devices with biometric reader (optional).

7.7.1   Call up and requirements

Software option

The "Local Enrollment" function is a software option. The function can only be entered if the required entry is available in the license file.

A function call up without corresponding license generates an O5 error record.

Disable and enable by the host

The "Local Enrollment" function can be enabled or disabled with the data records I2 and I3. The "Local Enrollment" function is enabled by default.

Function call up

The "Local Enrollment" function must be called up by a booking. The used function key must be set to limit value check "30".

Enroll PIN

To protect access to the biometric database in addition a Password is requested. The password can be set by using the parameter setting "Password parameter setting and customer number" (X02 record).

A password is not stored by default.

Timeout

If the user does not enter anything within 70 seconds, the "Local Enrollment" function is automatically closed.

i	Please see manual of the B-Client PDC6 terminal software for a detailed description of the parameter and data records named above.

7.7.2   Biometric management functions

After call-up, the system menu is displayed. The current assignment of the internal CBM database is additionally displayed. The example shows that the database contains 23 of 500 possible finger templates.

Please Select Function (C=Cancel)				
DB usage 23 of 500 entries used				
Enroll	Unenroll	List	Identify	Erase

The functions of the system menu are activated by means of the function keys below.

7.7.2.1   Enroll

This function serves for enrolling new individuals in the local database and for transmitting templates to B-COMM. The Enroll function can only be performed if a connection via the BCFTC stream has been established, otherwise the error text "No FTCS connection!" is displayed (not in standalone operation).

First it is checked if free space is available in the local database. If not, the message "Local database is full!" is output and an acoustic signal is emitted.

If there is space available in the local database, the user is requested to enter the template ID. The individual to be newly enrolled is identified by means of the template ID. The ID length is specified by the "PresetEnroll" parameter in the system.ini or by parameterized badge definition.

Press "Cancel" to cancel the entry and return to the menu. Press "OK" or the E button to confirm the entry.

If the ID already exists, the message "<Template ID> already exists" is output and an acoustic signal is emitted.

After entering the template ID, the actual enrollment process starts. Two fingers are enrolled and three images of each finger are taken.

To do so, each finger has to be briefly placed on the reader window three times.

The current finger (1 or 2) is shown in the display. The number of the image taken at the moment is shown in brackets. Successful recording of a finger is confirmed by means of a short acoustic signal. A quality value is specified for each enrollment process.

Example:

```
                    Enrollment
                   Finger 1 (1/3)
                   Quality: 103
```

Press "Cancel" to cancel the process and return to the menu.

If the finger position is not ideal during enrollment, corresponding symbols are shown on the display, see chapter 7.4.2.

If the finger is already recorded in the CBM reader database, the error message "Finger <X> matched! (<Template ID>)" is output and an acoustic signal is emitted.

At the end of the enrollment process, an overview with the following contents is displayed.

- Total quality of the enrolled fingers by means of text and figures.

- Belonging ID.

Example:

```
                    Enrolled ID: 00000126

               Template 1: 103 / Template 2: 96

                  Template quality:  good

        OK          Cancel        Retry
```

The quality of the enrolled fingers is subdivided into three levels.

•	> 120	Very good quality
•	60-120	Good quality
•	< 60	Poor quality

If the quality is poor, then the enrollment process should be repeated.

Wait for the new template to be collected by B-COMM (not in standalone mode). The message "Sending template to FTCS..." is displayed. The process will be continued as soon as B-COMM has collected the template (normally after 1-2 seconds).

If B-COMM is not available, the message "Timeout in connection to FTCS!" is displayed after 10 seconds and an acoustic signal is emitted. In this case, the generated template is not stored in the local database.

7.7.2.2 Unenroll

A specific template can be deleted from the database via its template ID using the Unenroll function (only in standalone operation).

The input ID is deleted by pressing "OK" or the E button. This is confirmed by an acoustic signal. In case of error, an acoustic signal is emitted and the message "<Template ID> does not exist!" or "Deleting template failed!" is displayed. Return to the menu in both cases or by pressing "Cancel".

7.7.2.3 List

This function lists all template IDs stored in the data base. The list can be scrolled using the arrow keys of the display keypad or the accordingly marked function keys (depending on terminal).

Press the C button to cancel the function and return to the menu.

7.7.2.4 Identify

This function allows identification of an individual. After calling the function, the finger has to be placed on the reader window. After successful identification, an acoustic signal is emitted and the corresponding ID is displayed.

Press "OK" to confirm the result and return to the menu.

The identified template can be deleted by selecting "Unenroll". The delete operation has to be confirmed afterwards.

If the finger position is not ideal during enrollment, corresponding symbols are shown on the display, see chapter 7.4.2. The finger position on the reader window has to be corrected accordingly.

In case of error, "Identification failed!" is displayed. Return to the menu.

7.7.2.5 Erase

The entire local biometric memory can be deleted by means of this function.

A code is requested for safety reasons. The Erase PIN is always "439235".

If a wrong code is entered, an acoustic signal is emitted and the message "Wrong Erase PIN!" is displayed. PIN input can be cancelled by pressing "Cancel" or the C button.

Deleting of finger templates out of the local biometric memory of the terminal is only useful in standalone mode. When comparing biometric data with B-COMM the finger templates are recovered automatically.

8   Maintenance

8.1   Buffer battery
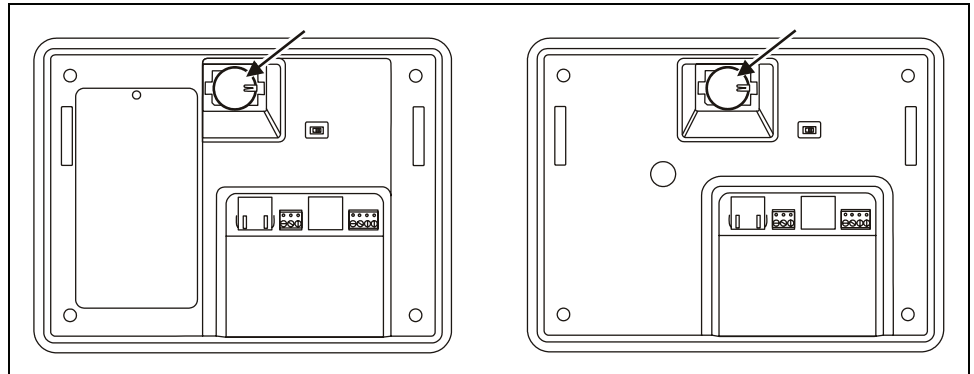
The device has a lithium manganese dioxide battery, type CR2032, to buffer the memory. The battery is on the rear of the terminal housing.

The buffer battery must be replaced by a new one every 2 years.

NOTICE!

Immediate data loss in the absence of buffering

If the battery is removed, with the terminal switched off, or if the battery is already empty at the time of switch-off, booking records, master records, profiles and the parameter setting will get lost immediately.

In this case, following the battery replacement, a cold start must be carried out, and then the data must be transferred again to the terminal.

•   Save all data, before switching off the terminal.

•   Perform the battery change with the unit switched on.

         To do so, use a PoE power injector, e.g., 04042778, for supplying power to the terminal. This injector must remain connected to the network connector of the terminal for the duration of the battery change.

8.1.1   Battery change

CAUTION

Lithium batteries can rupture or burst like an explosive.

Improper handling of lithium batteries can cause fire and explosions.

- Lithium batteries may only be replaced by the SERVICE PERSON.
- They may only be replaced by batteries of the same type.
- Do not open, bore through, or crush lithium batteries.
- Do not burn lithium batteries or expose them to high temperatures.
- Do not short-circuit lithium batteries.
- Do not recharge the lithium batteries.

1. Remove the terminal housing from the mounting plate.

2. Connect the PoE power injector to the network socket of the terminal, thus ensuring power supply of the terminal during the battery change.

3. **NOTE:** Do not use tools such as screwdrivers and the like.
   Remove the old buffer battery carefully by hand from the battery holder.

4. Press new battery into holder until it snaps into place.

5. Remove the PoE power injector.

6. Fasten the terminal housing to the mounting plate.

8.2   Replacing the UPS batteries

To ensure the function of the uninterruptible power supply, the UPS batteries must be replaced with new batteries every 3 years.

A set of replacement batteries consisting of 6 batteries can be purchased from Kaba under the order number 04043851.

Specification NiMH battery, 1.2 V, capacity min. 2000 mAh, size AA

NOTICE

Wrong battery types or incorrectly inserted batteries can overheat and damage the device.

- •   Use new identical batteries conforming to the above specification only.
- •   Do not use any primary battery cells.
- •   Ensure correct polarity.

- •   Remove the TORX8 screw (arrow).
- •   Remove the cover of the battery compartment.
- •   Remove old batteries.
- •   Press new batteries into the holding clamps.
- •   Re-attach cover.
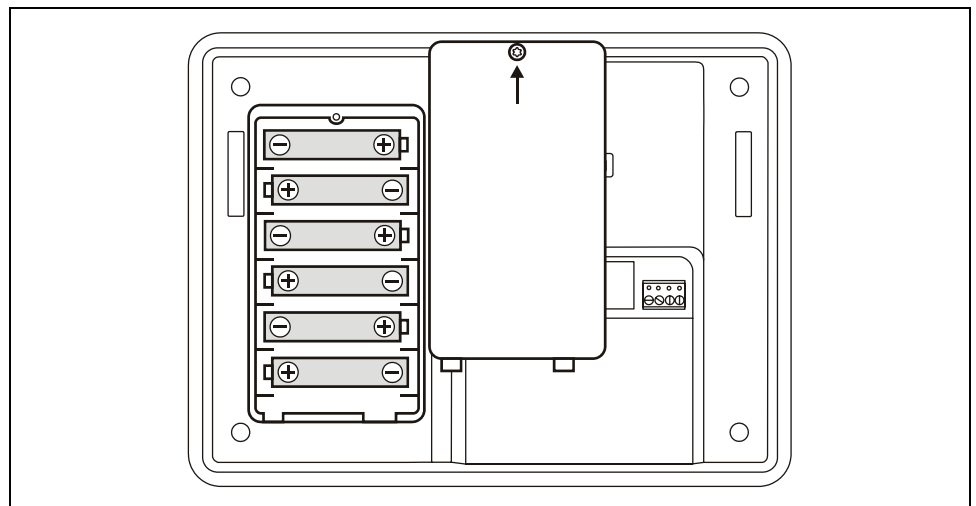
After an operating time of about 10 hours, the batteries are completely charged, and the UPS is ready for use.

Old batteries must be disposed of according to state and local regulations.

8.3   Cleaning the housing

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

Observe the following instructions in order to avoid producing damage to the housing and the reader window of the biometric reader (if any) during the cleaning process:

- Do <u>not</u> use alcohol, such as ethyl alcohol or isopropyl
- Do <u>not</u> use aggressive solvents
- Do <u>not</u> use cleaning agents with added powder
- Avoid scratching and abrasive movements

9   Packaging / returns

Not properly packaged components and devices can cause costs due to damages during shipping.

Please observe the following information when sending products to Kaba.

Kaba GmbH is not liable for products that have been damaged due to negligent packaging.

9.1   Complete devices

The original packaging has been specifically designed to fit the device. It offers maximum protection against damage in transit.

Always use the original packaging for returning the products!

If this is not possible, packaging which ensures that the device is not damaged during shipping and handling must be provided.

- Use a robust and thick-walled transport box or cardboard box. Approximately 8 to 10 cm of space needs to be allowed on either side of the device.

- Wrap the device with a suitable foil or put it into a bag.

- Generously stuff foam pads or air cushions, for example, all around device. Movements of the device inside the packaging must be excluded.

- Use only dustless and environmentally friendly padding material.

9.2   Electronic assemblies

ESD sensitive electronic assemblies such as printed circuit boards, readers, etc. must be stored, transported, and shipped in appropriate ESD protective bags.

Electronic assemblies may only be packed at ESD secure workplaces and by persons familiar with general ESD safety standards and who apply them on a regular basis.

Returning electronic assemblies in packaging with sufficient ESD protection is a prerequisite for

- the submission of warranty claims after functional failures of any type.

- replacement of printed circuit boards and electronic components in exchange.

Electronic components delivered in packaging without sufficient ESD protection are --in order to maintain a high quality standard-- neither analyzed nor repaired but directly disposed of.

9.3   Labeling

Complete return documents and a correct labeling allow for fast processing.

Please make sure that each package includes a delivery note. The delivery note should contain the following information:

- Number of devices or components per package.

- Product numbers, serial numbers, specifications.

- Name and address of your company / contact person.

- Reason for return, e.g. repair exchange.

- Meaningful and detailed error description.

Returns from countries outside the European Union require a customs invoice stating the real customs value.

Some countries (e.g. Switzerland) require a preference.

10   Disposal

This product complies with the WEEE directive and is, according to DIN EN standard 50419, marked with the "Crossed out garbage can" symbol. See chapter 3.4 Labeling.

The symbol refers to separated disposal of electric and electronic devices in EU countries.

Please do not dispose of device in your regular garbage.

Used devices contain valuable materials that should be recycled. Used devices should therefore be disposed of via your country's take back system.

At the end of use of the goods supplied, Kaba GmbH will take them back for a proper disposal in accordance with the legal regulations (German law on the disposal of electrical equipment (ElektroG)). Charges incurred for transport to the manufacturer will be at the expense of the owner of the waste electrical equipment.

In the EU and Switzerland, electronic devices have to be disposed of according to national disposal and environmental legislation.

Please dispose of in an environmentally responsible way.

The packaging materials are recyclable. Please do not throw packaging material into your regular garbage can. Always take it to a recycling center or have it picked up by your local waste recycler.

Lithium batteries

CAUTION

Lithium batteries can rupture or burst like an explosive.

Improper handling of lithium batteries can cause fire and explosions.

- Please store batteries to be disposed of carefully in order to avoid short-circuits, crushing, or damage of the battery housing.

See also chapter 2.4 Handling lithium batteries.

Used lithium batteries must be disposed of according to state and local regulations.

UPS batteries

In devices equipped with uninterruptible power supply UPS, NiMH batteries are used. Replaced batteries must be disposed of according to state and local regulations.

11   Index