SKIDATA®
KUDELSKI GROUP

# Keydetector.Gate ‘wall/desk’

Car Access
Instructions for Installation V1.1

www.skidata.com

Documentation & Training

**Instructions for Installation – Keydetector.Gate** ‘wall/desk’
June 2011 Edition

**SKIDATA AG**
Documentation & Training
Untersbergstrasse 40
A-5083 Groedig/Salzburg
Tel.: +43 6246 888-0
Fax: +43 6246 888-7
Internet: http://www.skidata.com
E-mail: docu@skidata.com



**Note**
Great care has been taken to make the information contained in this documentation as correct and accurate as possible. Although this documentation is updated regularly, SKIDATA AG cannot guarantee the absolute correctness and completeness of the information contained herein.

**Trademarks**
This documentation may contain representations of registered product or service trademarks owned by SKIDATA AG or third parties, as well as references to proprietary know-how protected by copyright laws or other legal provisions. In any case all rights remain exclusively with their respective owners.
SKIDATA® is a registered trademark of SKIDATA AG in the USA, the European Union and other countries.

**EU Directives**
All devices mentioned in this document were designed and manufactured in compliance with one or more of the following EU Directives:

Machinery Directive 98/37/EC
Machinery Directive 2006/42/EC
EMC Directive 89/336/EEC, as amended by 91/263/EEC, 92/31/EEC, 93/68/EEC
EMC Directive 2004/108/EC
Low Voltage Directive 73/23/EEC, as amended by 93/68/EEC
Low Voltage Directive 2006/95/EC
R&TTE Directive 1999/5/EC

**The following regulations apply expressly to all UL certified devices:**
If a device is retroactively converted, upgraded or otherwise modified, this automatically voids any existing UL certification of that device. UL certifications apply only to devices in their original condition that have been properly installed in accordance with the appropriate installation instructions and applicable local regulations.
To retain UL certification of a retroactively modified device, an "On-Site Certification" must be obtained from Underwriters Laboratories Inc. (UL) by and at the expense of the device operator.

# Table of Contents

# 1 About this documentation

This documentation contains **step-by-step instructions** for selected procedures required for the Keydetector.Gate ‘wall/desk’. It does not claim to be complete.

The procedures described in this manual do not include troubleshooting. In case of problems, please send an accurate problem description to SKIDATA AG Customer Service.

## 1.1 Print layout

For optimum printing, set your printer to **Color** and **Double-Sided** Printing.

## 1.2 Dimensioning

Dimensions in this documentation are always specified in **mm**. In cases where other dimension units are used, they are clearly indicated and specified separately.

## 1.3 Symbols

Important text passages and notes are marked by symbols and special typefaces throughout this Manual.

The following symbols are used:

**Danger:** Risk of injury.

**Danger:** Risk of injury by rotating parts. Do not touch any of these parts while the unit is running.

**Danger:** Risk of injury caused by heat. Do not touch any of these parts while the unit is running. Wait until they have cooled down before touching them.

**Danger:** Risk of electric shock. Do not touch these parts unless the power supply of the device has been disconnected.

**Danger:** Risk of radiation. Never point the laser at your or other person's eyes, whether directly or indirectly (by reflection). Laser radiation can cause irreparable eye damage.

**Danger:** Possible health risks from electromagnetic field. This applies to persons wearing pacemakers or other active or passive medical devices.

**Warning:** Electrostatically sensitive parts. Be sure to discharge any static electricity (e.g. by grounding yourself to a metal object or wearing an ESD wristband) before touching the device. This is to avoid possible ESD damage.

**Notice:** Warns against actions that might cause hardware and/or software damage.

**Hint:** Provides explanations on the proper use of the device or software.

**Example:** Describes practical applications to illustrate features, functions, etc.

# 2 Safety Instructions

Keydetector.Gate ‘wall/desk’ has been tested for safety. Operating personnel will be advised of possible residual danger during system training courses and by the information provided in this manual.

- System units may be used only for their intended purpose, as specified by the manufacturer.
- Unauthorized modifications of the units, as well as the use of replacement parts and/or add-on devices not approved by the manufacturer may lead to electric shock or cause other serious bodily harm and will void the manufacturer's warranty.
- The setup, installation, maintenance and configuration of the system units is limited to certified electricians with special training in the prevention of accidents.
- The technician or project manager responsible is to ensure that the unit is installed and configured in compliance with local technical guidelines as well as other applicable local regulations. Relevant parameters include (among others) cable dimensions, protection against risks, earthing, deactivation, disconnection, insulation testing and over current protection.

## 2.1 Risk of electric shock

Electrical repair work must be carried out by a professional electrician.

**Danger:** Electric installation and maintenance work may be carried out only by appropriately qualified, licensed electricians. Mains connections must be hard-wired. Please ensure full compliance with all applicable national and international rules and regulations concerning electric connections, as well as all applicable safety rules.

## 2.2 Electrostatic Discharge (ESD)

**Warning:** Electrostatic Discharge (ESD) energy can harm electronic components. Under certain conditions, ESD may build up on your body or an object (e.g., a peripheral device) and then discharge into another object. Be sure to discharge any static electricity (e.g. by grounding yourself to a metal object or wearing an ESD wristband) before touching the device. This is to avoid possible damage from ESD.

## 2.3 Warranty and liability

Except for all stipulated warranty and liability regulations, all warranty and liability claims shall be excluded, in particular if the harm or damage should be attributed to one or more of these instances:

- Misapplication (i.e., non-intended use) of the devices
- Improper installation
- Inadequate or missing warning and/or safety facilities in the danger area
- Irregular or insufficient maintenance
- Use of material not approved by SKIDATA AG
- Insufficient constructional renovation measures
- Insufficient training of operating personnel
- Unauthorized constructional, technical or other modifications of the system; Modifications and/or extensions of the system without the approval or explicit consent of SKIDATAAG
- Disaster situations brought about by impact of foreign bodies or acts of God

## 2.4 Electromagnetic Compatibility (EMC)

Compliance with Electromagnetic Compatibility must be maintained during operation. This requires that:

- Specified maximum lengths of network lines are not exceeded
- Network connections are properly installed and maintained
- Network cable screens are properly installed and maintained
- All system devices and facility installations that are subject to EMC regulations are inspected regularly and repaired if required

## 2.5 FCC Statement according to 15.19

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

## 2.6 FCC Note according to 15.21

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

## 2.7 FCC Statement according to 15.105

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.

## 2.8 Compliance Information Statement (Declaration of Conformity Procedure)

| | |
|---|---|
| Responsible Party: | SKIDATA, Inc. |
| Address: | 1209 W. North Carrier Parkway – Suite # 301<br>Grand Prairie, Texas 75050, USA |
| Telephone: | +1 (214) 204-1140 x207 |
| Type of Equipment: | RFID Reader |
| Model Name: | RD-KEYD/13MHz |
| FCC ID | QSS-RDKEY |

## 2.9 Canada Statement according to CNR-Gen Section 7.1.3

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:(1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

## 2.10 Canada Statement according to ICES-003 resp. NMB-003

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

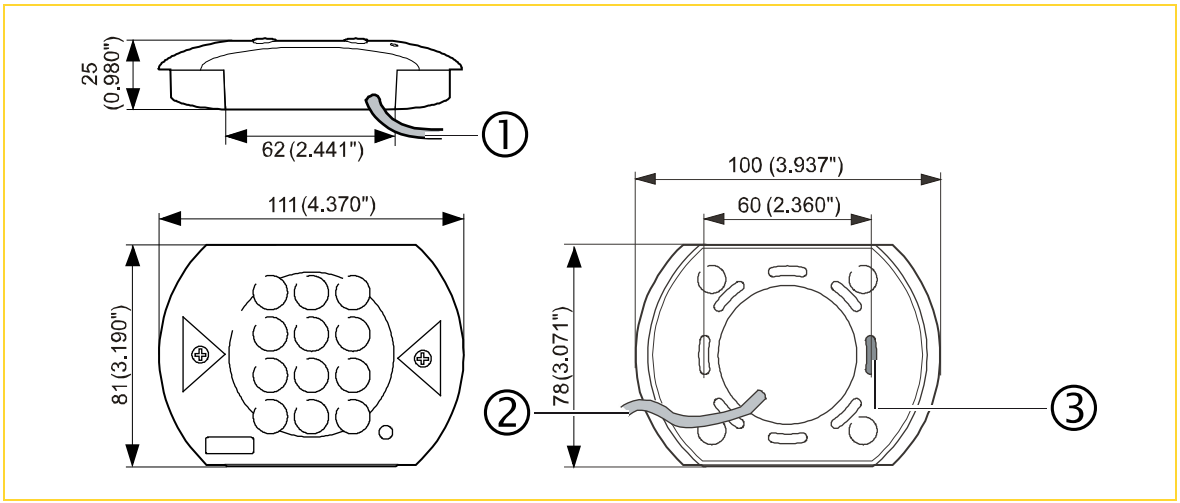
# 3 Technical Specifications

## 3.1 Keydetector

- Port: USB / SIO
- Supply Voltage: USB / SIO +5 V DC ± 5%
- Power Consumption: 2.5 W
- Scanning Range: keyard: approx. 80 mm (3.150")
- Reading Reaction Time: 0.2 secs
- Operating Temperature: +20 °C to +60 °C (-4 °F to +140 °F)
- Protection class: IP 44
- Mounting: As desktop version or in standard Ø 65 mm (2.559") wall socket
- Distance to metal objects: min. 5 cm (1.969")

## 3.2 Dimensions Keydetector.Gate

*Fig. 1: Dimensions Keydetector.Gate*




① Desktop version (cable length 3 m / 9.8 ft)

② Cable

③ Break out for mounting on standard wall socket Ø 65 mm (2.559")

# 4 Installation

The Keydetector can be used as desktop version or mounted in a concealed wall socket for solid or hollow walls, or surface-mounted next to the door.

**Notice:** In configurations supporting contactless access control technologies, avoid mounting the Door- / Gate Opener on a metallic surface, as this will reduce the scanning range (i.e. card/watch reading distance) of the unit considerably. When mounting the Door- / Gate Opener, a minimum distance of 5 cm (1.969") from metal objects must be maintained.

**Notice:** The control of inductive loads requires the use of a transzorb diode in reverse direction. Several Door Opener models are fitted with this diode by default.

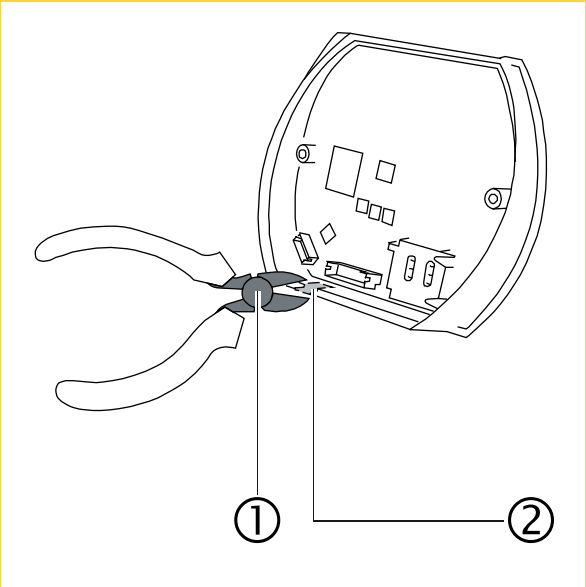
Verify that your Door Opener model is fitted with this diode (type: clamping diode 1N4007).

## 4.1 Desk-Mounting the Keydetector

**Notice:** The Keydetector comes factory pre-configured for wall mounting. Using the Keydetector as a desktop device requires some modifications.

- Remove break-off tab

*Fig. 2: Removing break-off tab*

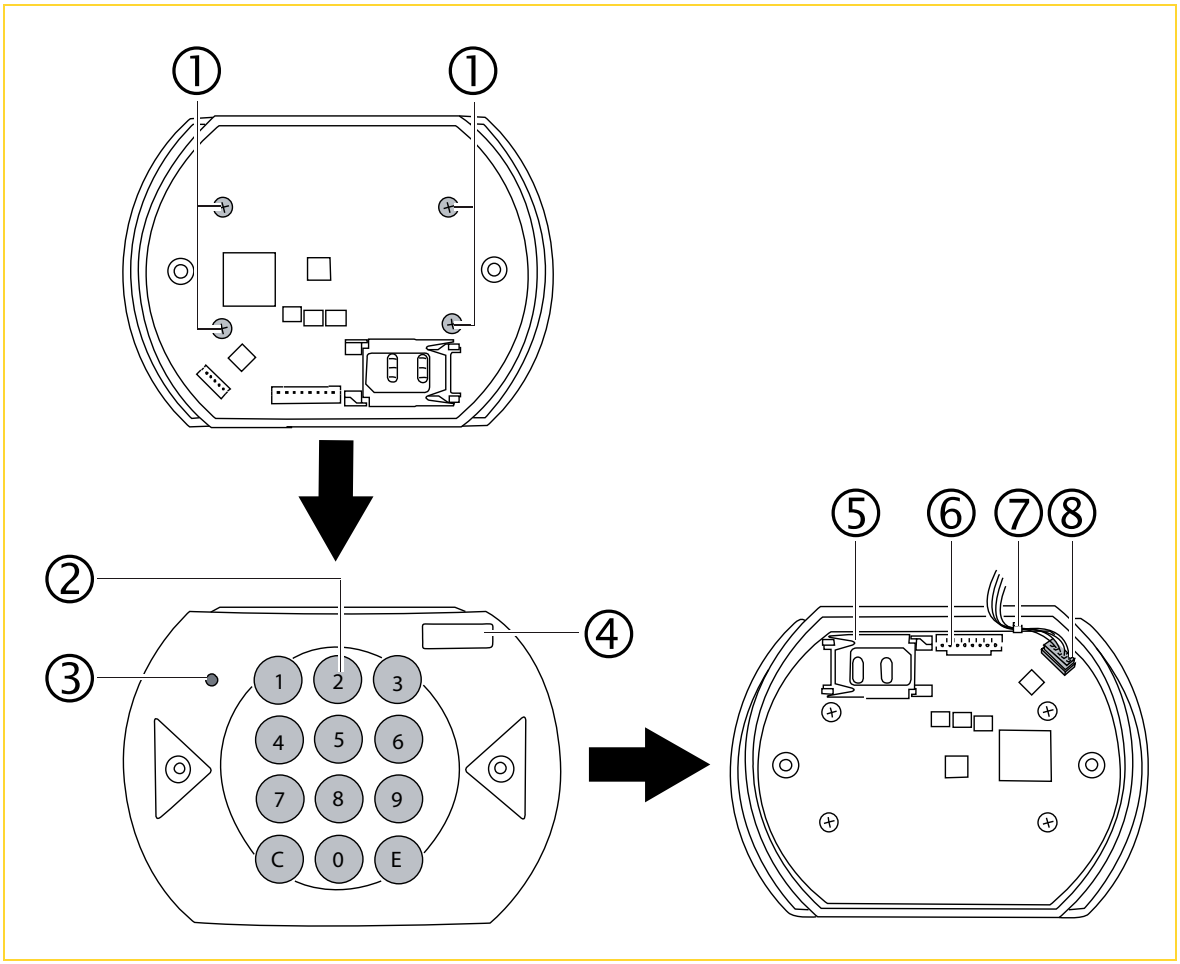



① Cutting device (e.g. side cutting pliers)

② Break-off tab

- Unfasten locking screws on the control board (PCB)
- Take out the sd804 board
- Take out the keypad, rotate it by 180° and reinsert it (the 1 key should now be next to the LED)
- Attach the SKIDATA label
- Screw the sd804 board into place
- Plug in the the USB connector and guide the cable through the hole where you removed the break-off tab

*Fig. 3: Unfastening screws, rotating keyboard, attaching label, plugging in USB connector*




① Locking screws

② Keypad

③ LED

④ SKIDATA label

⑤ SAM module

⑥ I/O connector

⑦ Cable ties for strain relief

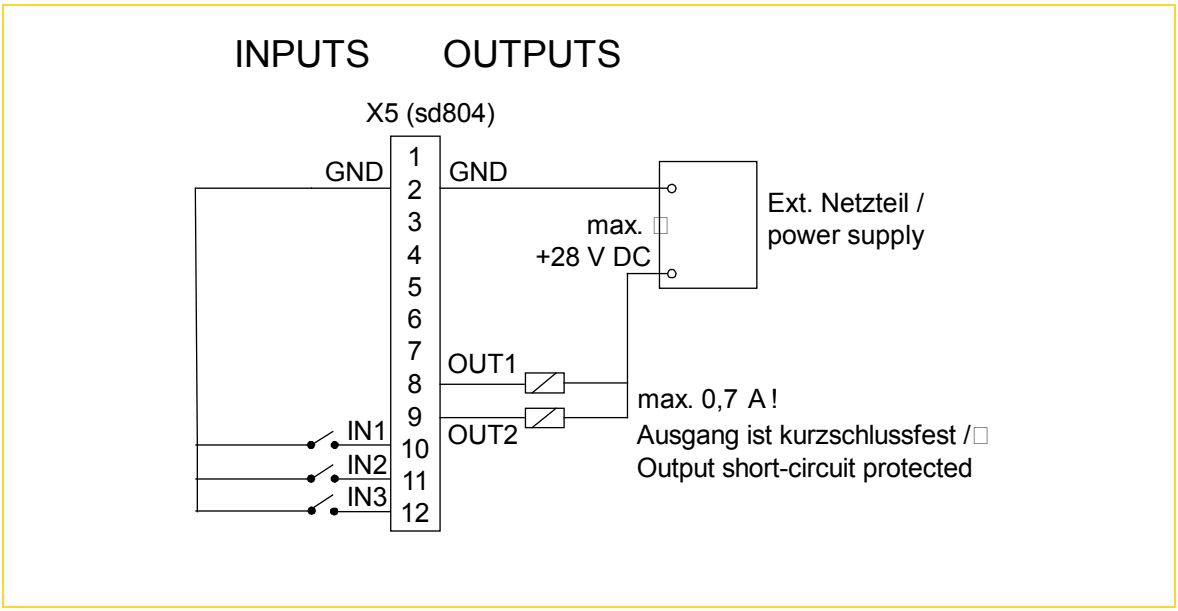
⑧ USB-connector

- If required, connect the I/O cable and use external relays to eliminate any electrical charge. (Open Collector)

*Tab. 1: Connections I/O cable*

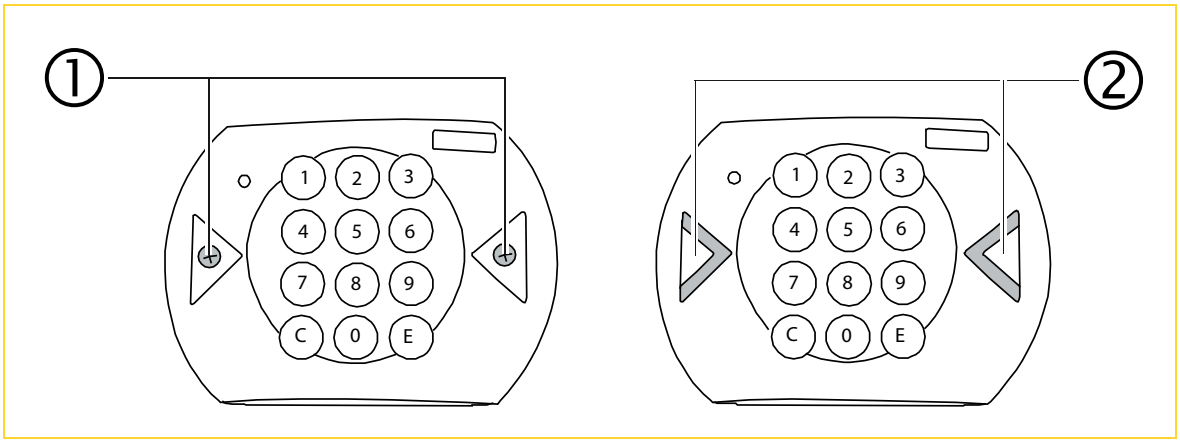
| Pin | Designation / Color |
|---|---|
| Pin 2 | GND (black) |
| Pin 8 | OUT1 (brown) |
| Pin 9 | OUT2 (red) |
| Pin 10 | IN1 (orange) |
| Pin 11 | IN2 (yellow) |
| Pin 12 | IN3 (green) |

*Fig. 4: Connections I/O cable*



- Close the casing and fasten the screws.
- Attach the arrow labels (default: yellow/gray, on demand: white/gray)

*Fig. 5: Phillips screws, arrow labels*



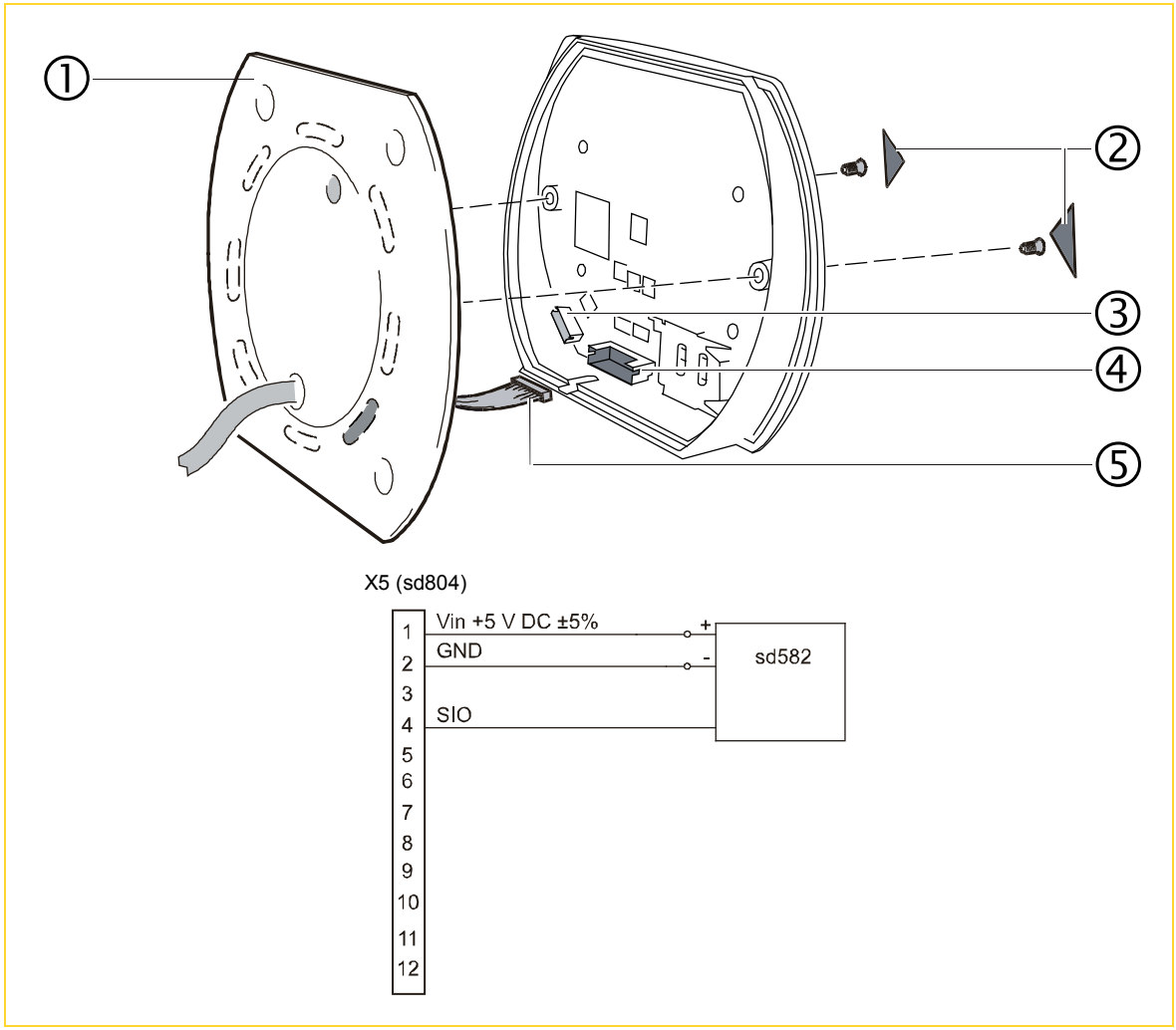

① Phillips screws ② Arrow labels

- Perform a functionality test: power on the device (plug into USB port on PC):the status LED should light up red.

## 4.2 Wall-Mounting the Keydetector with sd582

- Fix Skidata logo.
- Connect the Keydetector as illustrated.
- Fasten the rear wall onto the concealed outlet.
- Plug in SIO cable (3 m / 9.8 ft) (=power supply and data line from external controller)
- Place the housing on the Keydetector and tighten the fastening screws.
- Attach the enclosed masking stickers (Standard: yellow/grey; optional: white/grey).
- Switch on the unit to verify that the power supply LED is red.

*Fig. 6: Wall installation, Connections sd804*




① Rear panel Keydetector

② Fastening screws, Masking stickers

③ USB connector

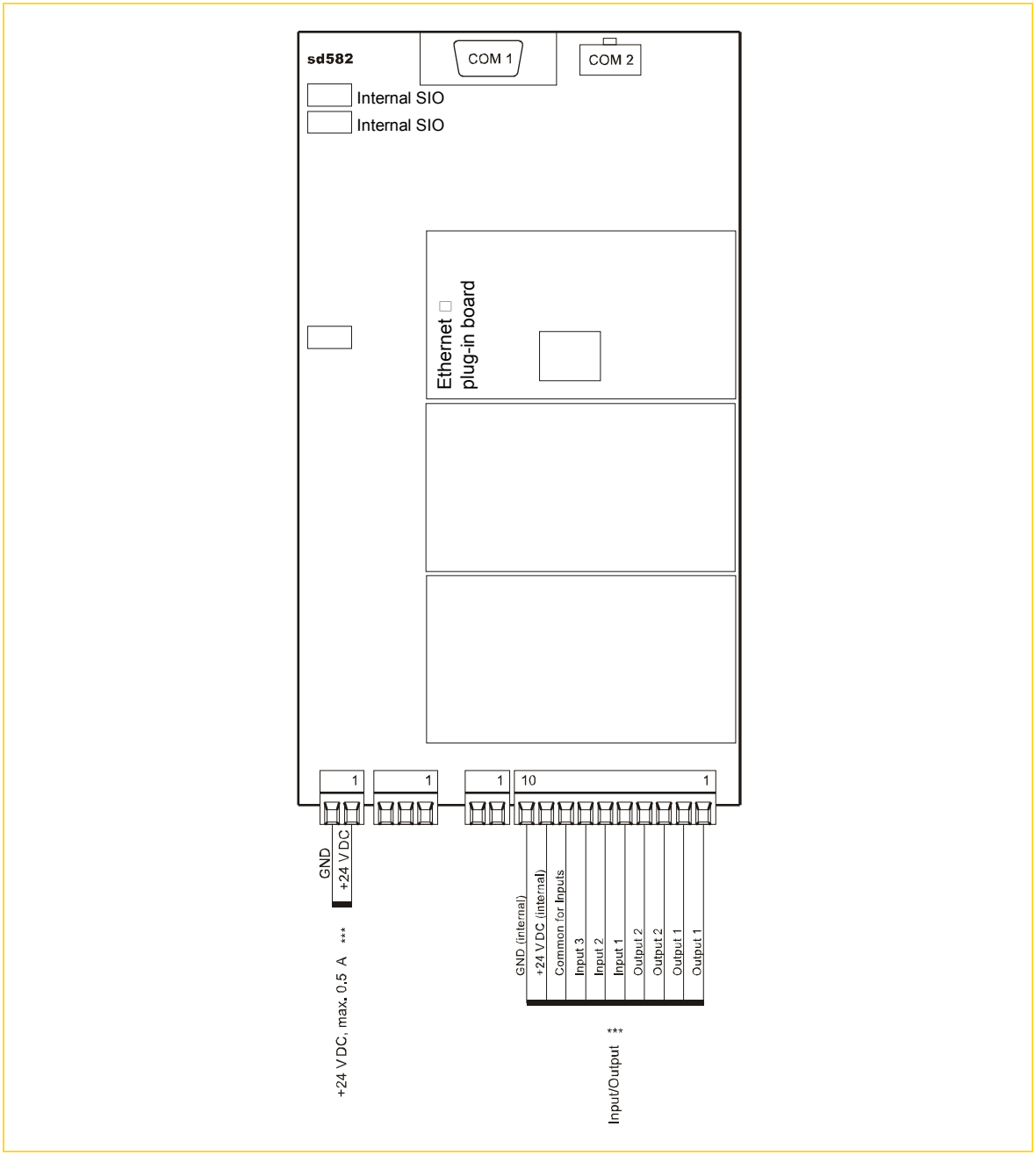
④ Connector power supply, data signals (SIO)

⑤ SIO cable (3m / 9.8ft)

### 4.2.1 Connecting to interface control card sd582

- Set up the cable connection to the Keydetector by means of the SIO cable (**Internal SIO** connector - see illustration)
- sd582 requires +24 V DC power supply
- Plug in Ethernet cable
- Connect door opener via I/Os

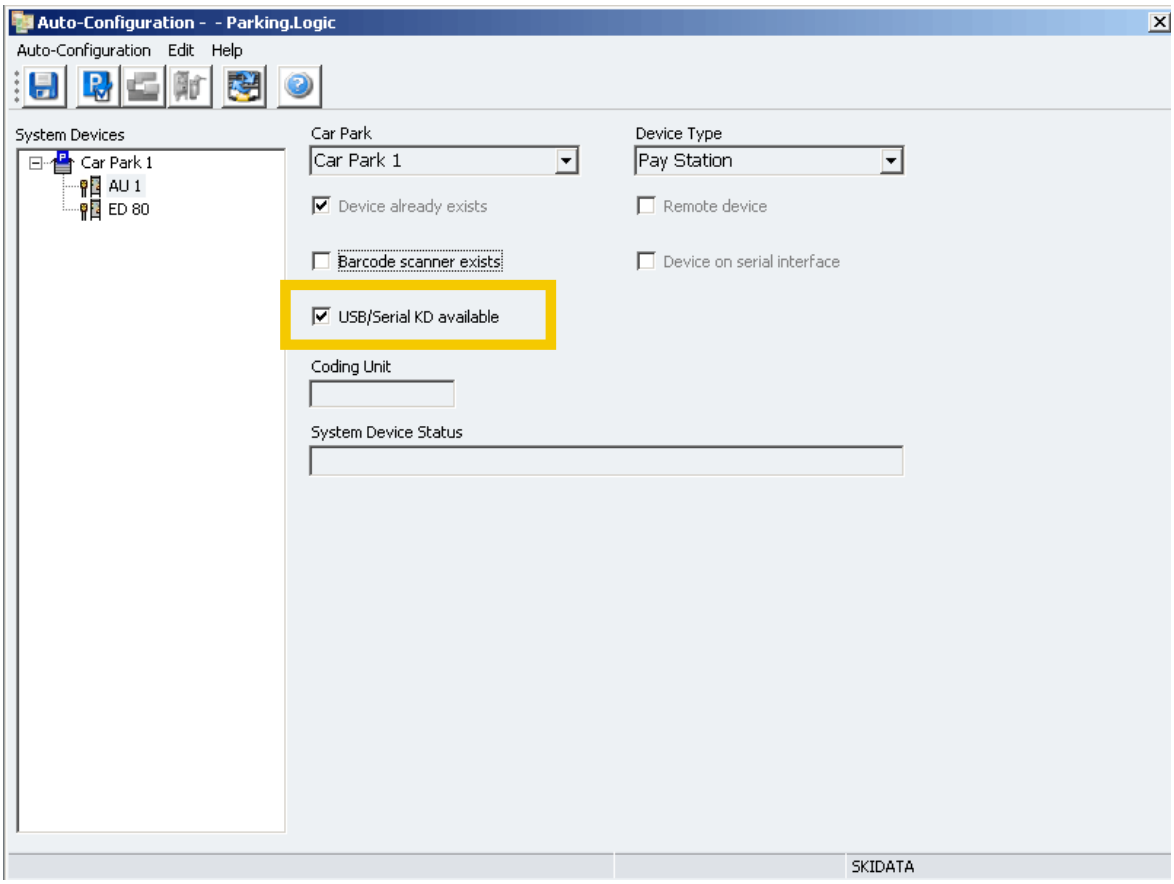
*Fig. 7: Connections sd582*



# 5 Integration into the system ('desk' version)

- Install the USB drivers
  (Release DVD: \Deploy\$OEM$\$1\Drivers\Ports\SDVCP\TicketReaderFamilyInstaller.exe)
- Select the **USB/Serial KD available** option
  (Main Menu>Automatic Configuration>System Devices)

*Fig. 8: Selecting checkbox*



# 6 Door- / Gate Opener

The Door- / Gate Opener allows for the automatic opening of doors and shutter gates by way of contactless reading of a keycard or Swatch Access watch (issued e.g. to contract parkers).

When using magnetic strip cards or barcode cards, a six-digit access code (printed on the card — see below) must be entered into the keypad of the Door- / Gate Opener.

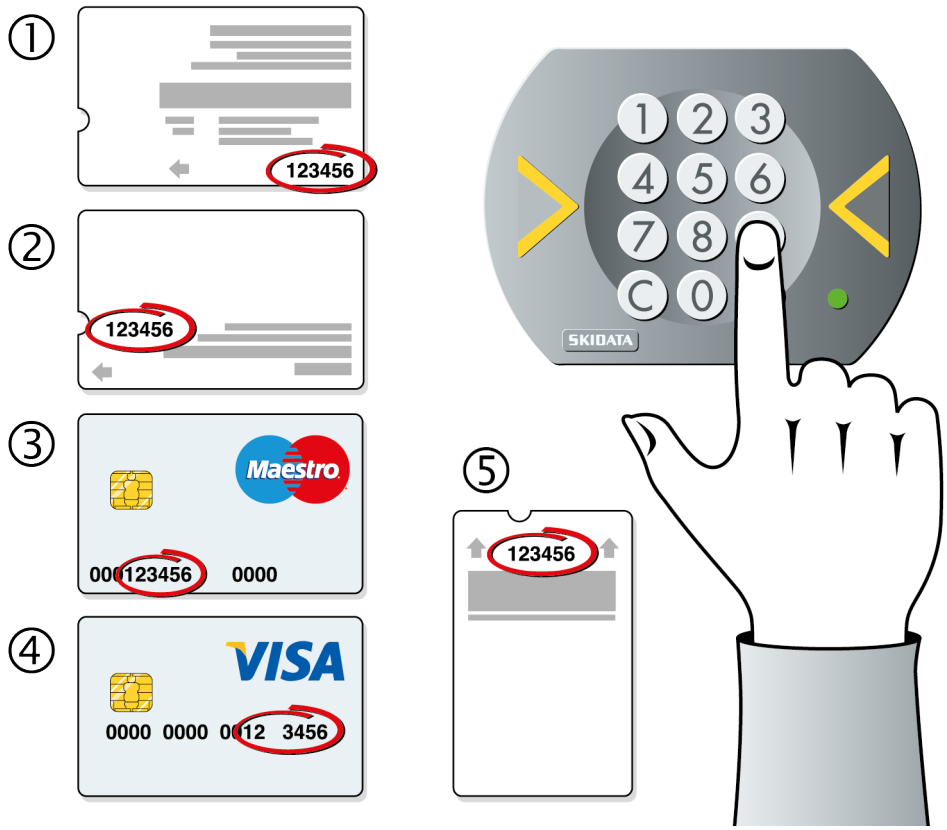
The access code of system-based cards (tickets) contains part of the facility number and a checksum (except for short-term tickets, which carry a serial number). The access code for credit card and ec-card holders consists of the last six digits of the card or account number.

The Door- / Gate Opener provides a cost-effective alternative to the Parking Column as an access control device for car park sections restricted to holders of contactless contract parking permits (keycard or Swatch Access).

Data transfer between the Door- / Gate Opener and the Administration Unit is effected by way of an sd448 serial interface converter. A separate control process is run for each Door- / Gate Opener (e.g. at the Admin Unit or a process computer).

The type and scope of the card verification process depends on the data carrier used.

*Fig. 9: Access Codes*




① Short-term parking ticket (lengthwise barcode)

② (Short-term) parking ticket with magnetic stripe

③ Ec-card

④ Credit Card

⑤ Short-term parking ticket (crosswise barcode)

**Tipp:** The schematic above is available as an adhesive (stick-on) pictogram (12 cm x13 cm). If only crosswise barcode tickets (5) and RFID tickets are used, the left section (1-4) may be cut off.

# 6.1 Card Verification Procedure of the Door Opener

## 6.1.1 Contactless Parking Products (keycard, Swatch Access)

**Normal Operation**

- Article Allowed
- Card Validity
- Time Window
- Transaction
- Card Blocked (i.e. access authorizations revoked)

**Emergency Mode** (if network connection between Administration Unit and Door- / Gate Opener is interrupted):

- Any readable contactless parking product is accepted.

## 6.1.2 Magnetic Strip Cards and Barcode Cards with Access Code

**Normal Operation**

- Personnel No.
- Checksum
- Facility No. (Access is also granted to holders of cards issued at permitted extraneous facilities.)

**Emergency Mode**

- Any 6-digit code is accepted

# 6.2 Card Verification Procedure of the Door Opener

## 6.2.1 Contactless Parking Products (keycard, Swatch Access)

**Normal Operation**

- Article allowed
- Card blocked
- Valid from
- Entrance Column, Pay Station or Automatic Payment Machine in Emergency Mode
- Door Opener in Neutral Mode (until 72 hours after activation of Neutral Mode)
- Presence

**Emergency Mode**

- Any readable contactless parking product is accepted.

### 6.2.2 Magnetic Strip Cards and Barcode Cards with Access Code

**Normal Operation**

- Personnel Card
- Is card blocked
- Is Card an Emergency Mode Ticket
- Presence

- If Entrance Column, Pay Station or Automatic Payment Machine is in Emergency Mode or Door Opener is in Neutral Mode (until 72 hours after activation of Neutral Mode) verify includes:
  - Checksum and
  - Facility No. (2 digits – Access is also granted to holders of cards issued at ‘permitted extraneous facilities’.)

**Emergency Mode**

- Any 6-digit code is accepted.

**Emergency Mode Ticket**

Access codes assigned to short-term tickets during emergency operation will be accepted after normal operation is resumed, and also after the vehicle has exited the car park.

## 6.3 Operational States

### 6.3.1 IDLE State (Door Opener Only)

The Presence Detection Loop is not vaporized; neither Keep Open nor Keep Closed is activated (via Control Centre); the LED is ORANGE; the Door- / Gate Opener is inactive.

### 6.3.2 Normal State

Gate Opener: The Presence Detection Loop is vaporized; neither Keep Open nor Keep Closed is activated (via Control Centre); the LED is flashing, its color alternating between GREEN and ORANGE.

Door Opener: The Presence Detection Loop input must remain in vaporized state (this can be effected by means of a wire link).

Keyboard an BLL-unit are activated; the LED is flashing, its color alternating between GREEN and ORANGE.

### 6.3.3 Out of Order

The unit has been deactivated (either manually via the Control Centre (Keep Closed) or automatically as the result of a fault); the keyboard and Contactless Reader unit are deactivated; the LED is RED.

Synchronization commands transmitted from the Administration Unit (Control Centre, system maintenance programs) are accepted.

## 6.4 Keypad

When the keypad is activated, a brief beep (click) is sounded every time a key is pressed.

Following the input of six consecutive digits, a beep lasting approximately one second is emitted to signal the completion of the code input. The code entered is then processed and the keypad buffer cleared.

If the delay between the input of the individual digits exceeds five seconds, the keypad buffer is cleared automatically, requiring the input procedure to be restarted. Users can also cancel their input by pressing the C or E key.

## 6.5 Data Exchange with Control Centre Program (CTC)

### 6.5.1 Door- / Gate Opener

When the Open command is issued, the Door- / Gate Opener output terminal is activated for a pre-defined period (this can be adjusted via the Device Settings program).

The LED lights up GREEN for three seconds, and a short beep is emitted. The unit then returns to Normal State.

### 6.5.2 Keep Open

The Door- / Gate Opener output terminal is permanently activated. The LED lights up GREEN. This state can be deactivated via the Keep Open OFF command.

### 6.5.3 Keep Closed

The system behavior is the same as when set to Out of Order.

### 6.5.4 Transaction NEUTRAL

Gate Opener: The gate opens even if the previous transaction with a contactless parking product was unsuccessful (e.g. if a card is used to gain access although it is already registered as being present).

Door Opener: Access is granted even if the card used is not registered as being present.

### 6.5.5 Display of Reason for Rejection

Shows a list of unsuccessful access attempts and the respective reasons why access was denied (e.g. Incorrect code entered, Card read error, Card not registered as present, etc). The list can be viewed via the Control Centre program of the Administration Unit.