

Operating instructions

HISAC[®]-RFID-Reader

Art. No. 301000.0, 301001.0, 301002.0

301000.0



301001.0



301002.0



Table of contents

1	Features	5
1.1	Intended use	6
1.2	Security	6
2	Scope of delivery	8
3	Technical data	9
4	Drawing	10
5	Product description	12
5.1	Touch function	12
5.2	LED display	12
5.3	Label	13
6	Assembly	14
6.1	Mechanical installation	14
6.1.1	Self-locking rubber grommet	14
6.1.2	Threaded nut	14
6.2	Buzzer	14
6.3	Installation in a metal wall	14
6.3.1	Installation of the glass version in a metal wall	15
6.3.2	Installation of concealed mounting in a metal wall	15
6.4	Dismantling	17
7	Electrical connection	18
7.1	Wire assignment	18
7.2	Bus-Select	18
7.3	LED input	19
7.4	Touch output (NO-contact)	19
8	Serial interface	20
8.1	CAN	20
8.2	Wiegand	21

9	Background information on DESFire AES support.....	22
9.1	Configuration requirements	22
9.2	Behavior with activated AES.....	22
9.3	Creating DESFire cards.....	22
9.4	Save AES Application ID and AES Masterkey on reader.....	22
10	Background information on NFC support.....	23
10.1	Preparation for HISAC® -RFID reader and enrollment	23
10.2	Smartphone preparation.....	23
10.3	Enrollment.....	23
10.4	Authentication.....	24
11	Procedure in the event of a malfunction	25

Disclaimer

© Copyright BSS Baumann Sicherheitssysteme GmbH 2025

All rights reserved.

Passing on and reproduction of these documents, utilization and communication of their content is not permitted unless expressly granted. Infringements will result in compensation for damages. All rights reserved.

We have checked the contents of this publication for conformity with the components described. However, deviations cannot be ruled out, so we cannot guarantee complete conformity. The information in this publication is checked regularly and any necessary corrections are included in subsequent editions.

We are grateful for any suggestions for improvement.

We reserve the right to make technical changes.

Trademark

HISAC® is a registered trademark of BSS Baumann Sicherheitssysteme GmbH.

Operating instructions valid for:

Item no:	30100x
Firmware:	V205 and higher
Document version:	1.2
Date:	15. April 2026

Version	Remarks / Changes	Date
V1.1	Bus select adapted to HD-Lock (firmware V119, bootloader V11)	28.11.2022
V1.2	- Firmware v205 and higher - Information on DESFire AES added - Supplement section Dismantling - Revision of texts - Supplement Wiegand - Installation: Ø27+/-0.2 changed to Ø27-0.2 - Integration of system integrator documentation into this document	15.04.2026

1 Features

HISAC® stands for "Highly Innovative Smart Access Control". The HISAC® RFID reader (Radio Frequency Identification Reader) with touch function is intended for use as an access control unit and optionally as an electronic button and door opener in the maritime sector.

HISAC® impresses with its compact design and simple installation options. This means that a simple hole drilled in the side wall into which HISAC® can be inserted is sufficient. No screws are required to install HISAC® securely and sealed.

HISAC® works with 125 KHz Hitag2 cards or tags and 13.56 MHz Mifare DESFire cards or tags. Optionally, AES encryption can be used for Mifare DESFire cards.

The HISAC® with glass front also has a touch function, i.e. when the glass surface on the front is touched, an electrically isolated contact closes for the duration of the touch.

An acoustic detector and an RGB LED are available as feedback elements for RFID detection and the touch function.

Communication with the higher-level evaluation unit is possible either via a CAN or Wiegand interface.

Features of the RFID reader:

- Power supply 12 VDC or 24 VDC
- RFID frequencies: 125 KHz and 13.56 MHz
- RFID read distance: $\leq 40\text{mm}$, depending on the installation situation and the RFID frequency used
- LED display
- AES encryption possible
- Touch function with galvanically isolated output (only with 301000.0)
- Selection of CAN or Wiegand protocol
- Compact design
- Simple assembly
- High degree of protection and seawater resistance when installed
- Cable length 7 m

1.1 Intended use

The HISAC®-RFID-Reader is intended exclusively for the identification and authentication of transponders (RFID media) in the intended frequency range. It is used for the contactless reading of RFID data and the transfer of this information to a higher-level control unit or evaluation unit. It is typically used in access control systems or similar applications in indoor or protected outdoor areas.

The reader may only be operated in conjunction with suitable transponders approved by the manufacturer and in accordance with the technical requirements and installation specifications described in these instructions.

Any other use, in particular use outside the specified electrical and mechanical framework conditions, is considered improper use. The manufacturer accepts no liability for any resulting damage.

1.2 Security

The following safety instructions must be observed when handling the HISAC®-RFID-Reader to prevent personal injury and damage to property and to ensure trouble-free operation:

General safety instructions

- The reader may only be installed and put into operation by qualified personnel.
- The power supply must be completely disconnected before installation, maintenance or removal.
- Only original components and accessories may be used.
- The applicable electrical safety regulations and regional installation standards must be observed.

Environment and installation situation

- The device may only be operated within the ambient conditions specified in the technical data.
- Installation in the immediate vicinity of metallic surfaces or strong electromagnetic fields can impair the function and should be avoided.
- For installation, the specifications described in the "Dimensions" and "Installation" chapters must be strictly observed.

Operation and maintenance

- The reader is maintenance-free. In the event of visible damage or malfunctions, the device must no longer be used.
- The housing and electrical connections must not be opened or modified.
- Cleaning may only be carried out with a dry, soft cloth when the power supply is switched off. Do not use aggressive cleaning agents.

Disclaimer

The manufacturer accepts no liability for non-compliance with these safety instructions, improper installation or improper use. In these cases, any guarantee or warranty claims are also void.

Important information and notes are marked below with the following symbols:



Information



Important note

2 Scope of delivery

- HISAC®-RFID-Reader
- Pre-assembled rubber grommet
- Hexagon nut for fastening
- Spacer ring (only for 301000.0)
- Operating instructions

3 Technical data

Approvals	CE
RFID frequencies	125 KHz and 13.56 MHz
RFID read distance 125 kHz ¹	approx. 20 mm
RFID read distance 13.56 MHz ¹	approx. 30 mm
Nominal operating voltage / voltage range	12 VDC or 24 VDC / 11...30 VDC
Power consumption in boot mode, LED and sound	max. 150 mA / 24 VDC max. 150 mA / 12 VDC
Power consumption when reading card (Mifare with AES), with sound	max. 200 mA / 24 VDC max. 250 mA / 12 VDC
Load capacity of the floating output	30V, 300 mA
Operating temperature / storage temperature range	-15 °C ... +60 °C / -20 °C ... +70 °C
Protection class	IP67 (front side, when installed)
Housing dimensions	See product drawing
Weight with connection cable	approx. 0.4 kg
Cable length	7 m with open end
Housing material	PC-ABS

¹ Depending on the installation situation and the type of RFID used.

4 Drawing

The following information on the dimensions serves as a basis for the correct integration of the device into the respective installation situation.

301000.0: HISAC® -RFID reader, with touch function, glass front

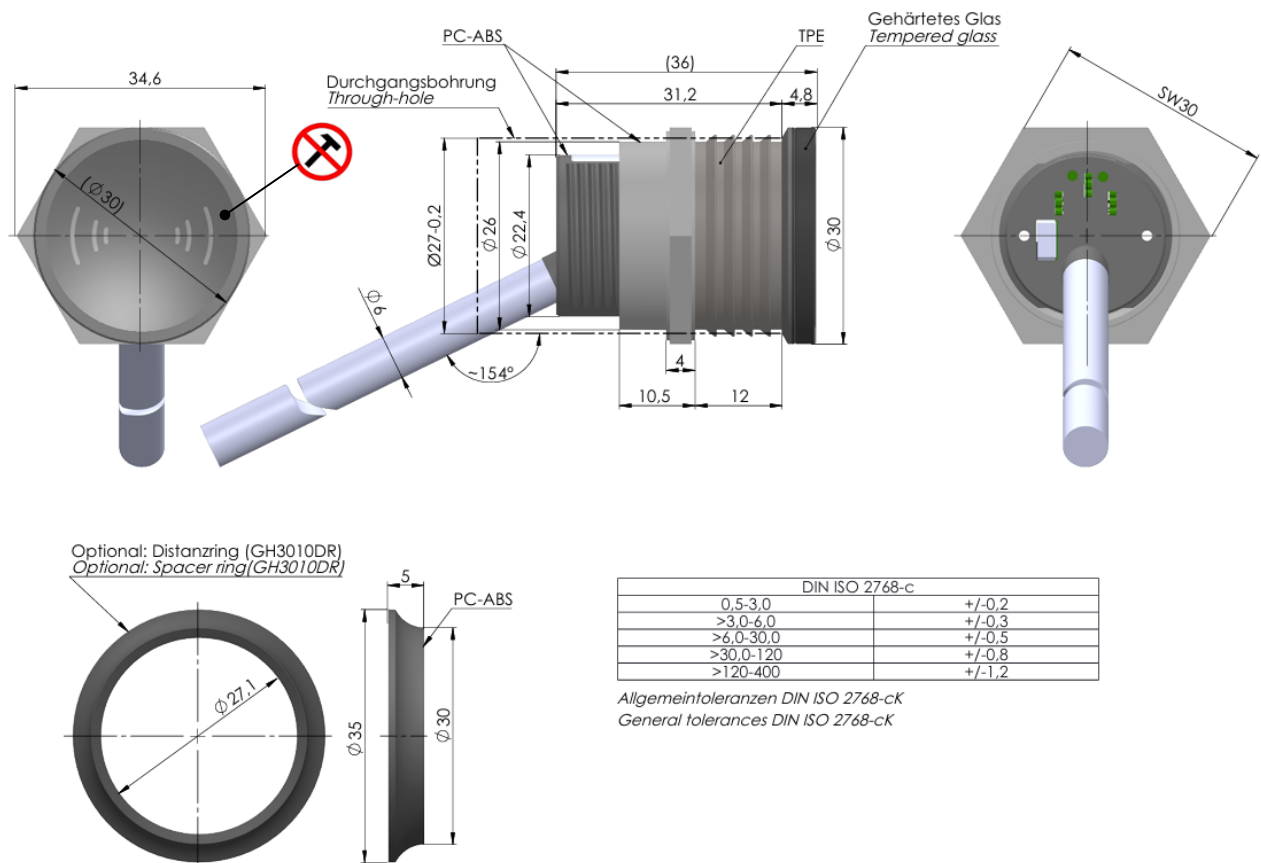


Figure 1: Product drawing HISAC® 301000.0

301001.0: HISAC® -RFID reader, VM, without touch, acrylic glass (frosted glass)

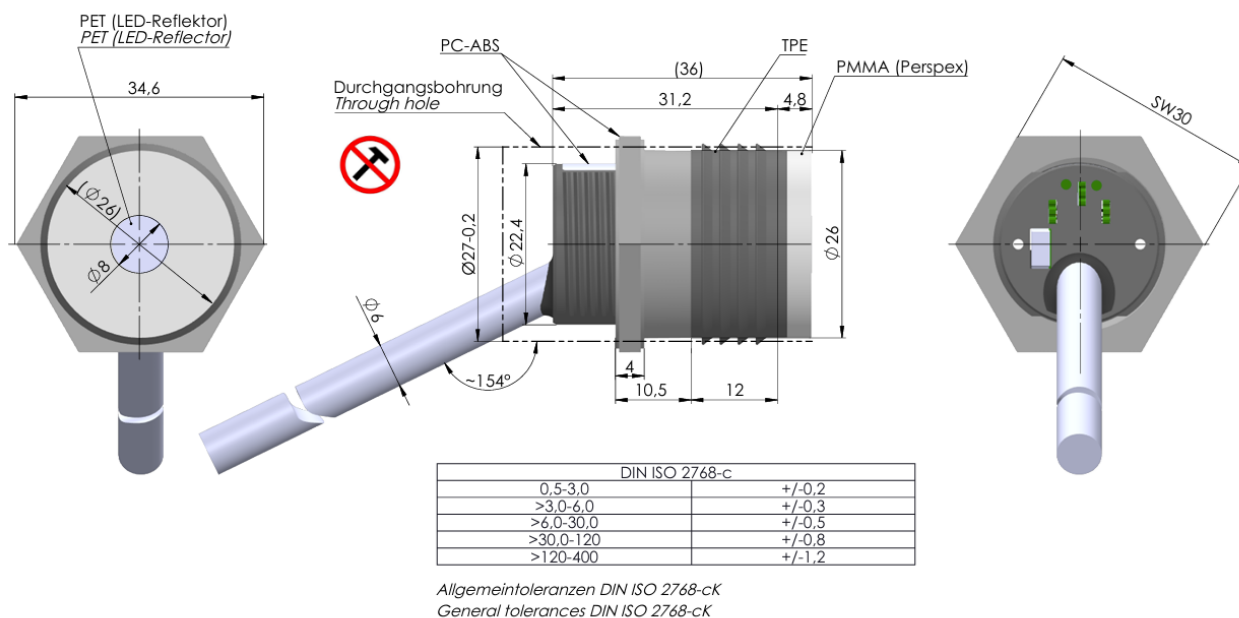


Figure 2: Product drawing HISAC® 301001.0

301002.0: HISAC® -RFID-Reader, VM, without touch, PE-100 (black)

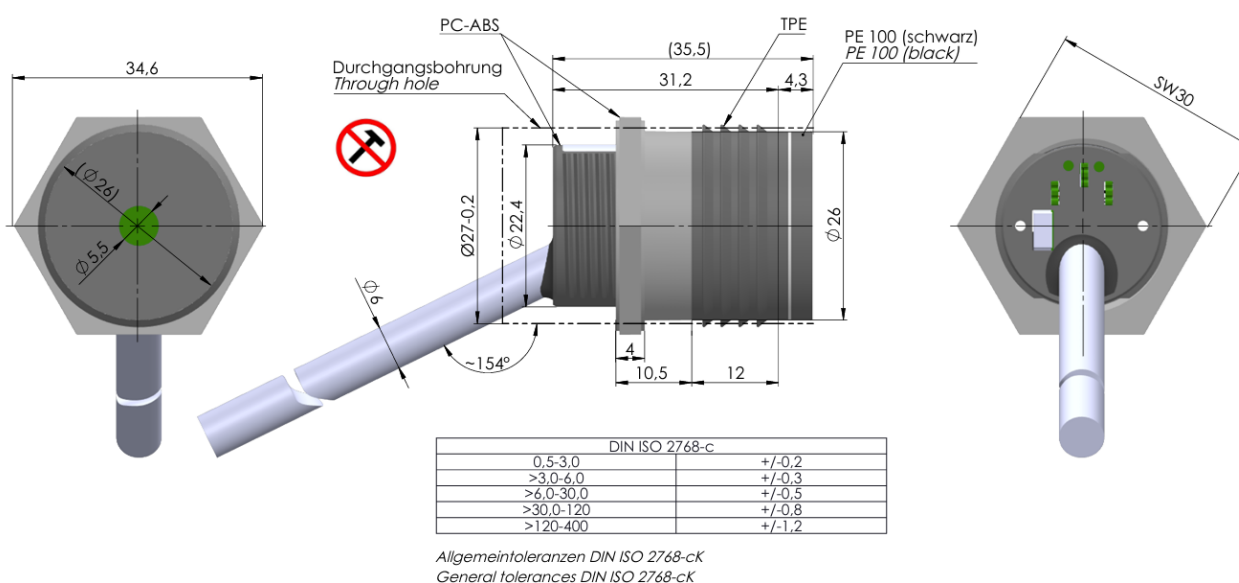


Figure 3: Product drawing HISAC® 301002.0

5 Product description

5.1 Touch function

A capacitive touch field is integrated in the center of the glass front of the HISAC® 301000.0. This is used for precise and user-friendly interaction with the device.

The HISAC® variants intended for concealed installation do not have a touch panel.



Figure 4: Touch panel HISAC® 301000.0

5.2 LED display

The HISAC® RFID reader is equipped with an LED display on the front. This LED can be controlled either via the CAN bus or via the reader's inputs to indicate various operating states.

The HISAC® RFID reader 301000.0 has a glass front with six circular segments:



Figure 5: LED display HISAC® 301000.0

The HISAC® -RFID-Reader 301001.0 has an illuminated plastic frosted glass:



Figure 6: LED display HISAC® 301001.0

The HISAC® -RFID-Reader 301002.0 is equipped with a black plastic disk that integrates an LED in the middle:



Figure 7: LED display HISAC® 301002.0

5.3 Label

The reader is supplied from the factory with a label containing important product information (e.g. firmware, serial number). This label must not be removed or damaged.

6 Assembly

The assembly of the HISAC® is a crucial step to ensure its optimal functionality. It is important to follow the instructions carefully and have all the necessary components and tools ready. Be sure to consider the environment in which the device will be installed, as certain conditions, such as metallic surfaces, may affect performance. Ensure that all electrical connections are made correctly and safely to ensure reliable and safe use of the appliance.

6.1 Mechanical installation

Two mounting methods are available for installing the reader, which can be selected flexibly depending on the location and structural requirements.

6.1.1 Self-locking rubber grommet

- a. Drill Ø27-0.2 mm hole.
- b. Slide the rubber grommet onto the reader housing.
- c. Insert the reader and cable into the hole from the front and press in.

6.1.2 Threaded nut

- a. Drill through hole.
- b. Insert the reader and cable into the hole from the front.
- c. Secure on the back with the threaded nut.



Hammer blows on the device are not permitted.

6.2 Buzzer

The buzzer is located on the back of the reader. When installing, ensure that there is sufficient space so that the buzzer remains clearly audible. Inadequate positioning can impair the acoustic perception of the buzzer and thus limit the functionality of the device.

6.3 Installation in a metal wall

If possible, install the reader in a non-metallic environment to ensure the optimum reading range. If installation in a metallic environment is unavoidable, use the supplied spacer ring to increase the distance to the metal or observe the subsequent installation in a metallic wall. Please note, however, that metal can affect the performance of the reader and reduce the reading range.



Installation in a metallic environment can significantly impair the reading range and, under certain circumstances, completely eliminate the functionality of the reader. It is therefore recommended to check the reading range after installation and make any necessary adjustments to ensure optimum functionality.

6.3.1 Installation of the glass version in a metal wall

For installation in a metal wall (e.g. steel, aluminum), a recess with a diameter $\geq \varnothing 120$ mm and a depth of ≥ 16 mm must be created.

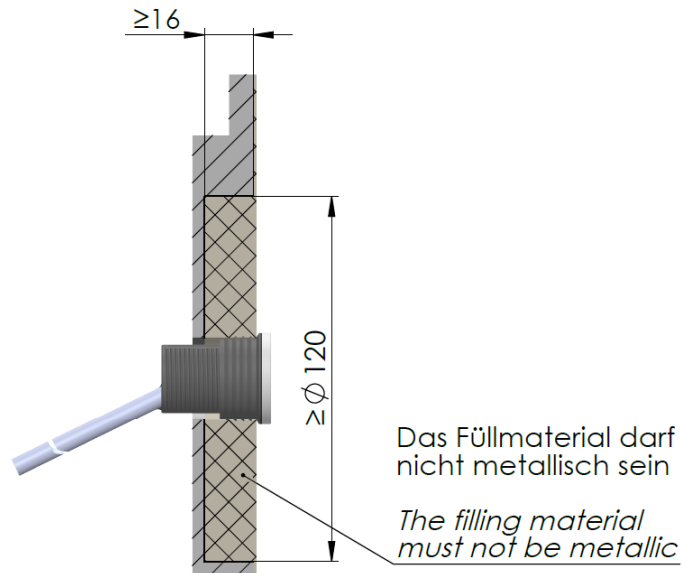


Figure 8: Installation in a metal wall for HISAC® 301000.0

The recess must be filled with a suitable, non-metallic material. This material must allow the creation of a centrally positioned locating hole with a diameter of $\varnothing 27-0.2$ mm.

6.3.2 Installation of concealed mounting in a metal wall

There must be no metallic materials in the direct vicinity of the device. For this reason, a recess with a diameter of at least $\varnothing 120$ mm must be provided on the installation side. The depth of the recess must be selected so that the remaining wall thickness in front of the device is a maximum of 2 mm. This ensures an optimum RFID reading range.

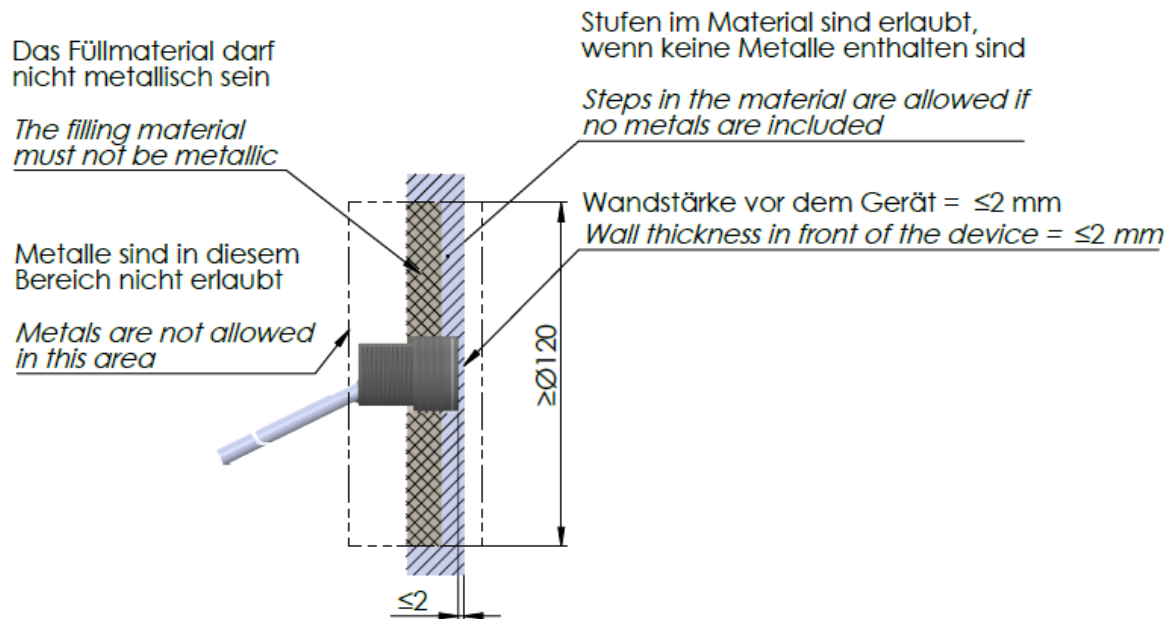


Figure 9: Installation in a metal wall for HISAC® 301001.0 and 301002.0

The recess must be filled with a suitable, non-metallic material. This material must allow the creation of a centrally positioned mounting hole with a diameter of $\text{Ø}27-0.2$ mm. The use of a light guide is recommended for optical feedback.

The following installation position must be selected for the positioning of a light guide:

Der Lichtleiter muss in einem Radius $R8,5 \pm 1,5$ mm außerhalb der Mitte positioniert werden.

The light guide must be situated out of the center with a radius of $R8,5 \pm 1,5$ mm.

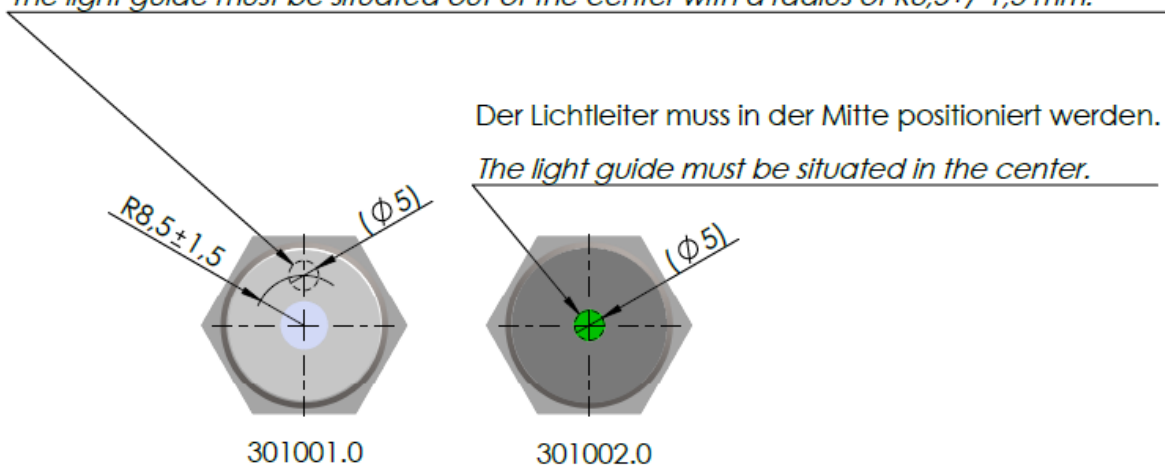


Figure 10: Light guide position for HISAC® 301001.0 and 301002.0

6.4 Dismantling

When removing the HISAC®, make sure that no pressure or tensile force is exerted on the front glass. Instead, the force should only be applied to the plastic housing to enable it to be pushed out. This ensures that the front glass remains undamaged and the functionality of the device is not impaired. Care should also be taken to ensure that no sharp tools are used that could damage the housing or the glass.

7 Electrical connection

The electrical connection is an essential step to ensure proper function. It is important to follow the connection instructions exactly and ensure that all connections are made correctly and safely. Make sure to use the correct cables and connections and check the polarity to avoid damage to the device. Ensure that the power supply meets the requirements of the appliance and that all safety precautions are taken to ensure a safe installation.

7.1 Wire assignment

No.	Wire color	Signal	Description
1	red	12V/24V DC	Supply voltage
2	brown	LED red	LED input red
3	white	LED blue	LED input blue
4	green	LED green	LED input green
5	blue	GND	Zero potential (supply voltage and the LEDs)
6	gray	RXTX-P/D1	CAN bus high internally connected to RXTX-P2 /Wiegand Data1
7	pink	RXTX-N/D0	CAN bus Low internally connected to RXTX-N2 /Wiegand Data0
8	violet	RXTX-P2	CAN bus high internally connected to RXTX-P
9	black	RXTX-N2	CAN bus Low internally connected to RXTX-N
10	yellow	Bus-Select	Bus select (Wiegand/CAN/BusOff)
11	gray/pink	Switch-1	Potential-free output (normally open contact). Connects to Switch-2 when the surface of the reader is touched.
12	red/blue	Switch-2	Potential-free output (normally open contact). Connects to Switch-1 when the surface of the reader is touched.
Shield	-	-	Connected to protective circuit and must be hung up.



If stranded wires are not required, ensure that short circuits are avoided.

7.2 Bus-Select

The interface of the HISAC®-RFID-Reader can be defined via this input:

- If the bus select input is switched to supply voltage potential, the CAN interface is activated and Wiegand is deactivated. The LED inputs are also deactivated (the LED is controlled via CAN).
- If the bus select input is switched to GND, the Wiegand interface is active and the CAN interface is deactivated. The LED inputs are also activated.
- If the bus select input is not connected, only the LEDs are active.

The potential-free output is always active.

When booting HISAC®, the Bus-Select is reported as follows:

CAN	3 x beep (long) + blue LED
Wiegand	5 x beep (short) + green LED
Bus off	1 x beep (long) + red LED

7.3 LED input

In "Wiegand-" and "BusOff-"mode, the inputs (red LED, blue LED, green LED) are active. If the voltage is greater than 2.5 V or less than 0.35 V, the respective RGB LED lights up. If the inputs are not connected, the LEDs remain switched off.

In CAN mode, the LEDs are controlled via the CAN protocol.

7.4 Touch output (NO-contact)

When the touch surface is touched, a connection is established between Switch-1 and Switch-2. Without touching, the two outputs remain separated from each other. The maximum permissible continuous current is 0.3 A, the maximum voltage between Switch-1 and Switch-2 is 30 VDC.

8 Serial interface

Commissioning the reader is a crucial step to ensure that it works correctly and efficiently. Start with a thorough check of all installation steps and make sure that all connections have been made securely and correctly.

Test all functions of the device to ensure that it is working properly. In the event of problems or irregularities, consult the troubleshooting section in this manual or contact technical support.

The HISAC® has the option of communicating either via Wiegand protocol (1 KHz) or via CAN bus protocol. The protocol to be used is defined via the bus select line at the time of switch-on - see chapter 7.2.

Further information on the protocols can be found in the separately available description of the interfaces.

8.1 CAN

When the CAN interface is selected, the HISAC® listens on the CAN interface for one minute after the operating voltage is applied to enable a firmware update. This is indicated by the continuous blue light of the LED.

The HISAC® can then be parameterized via the CAN 2.0B protocol. The following factory settings apply to this protocol: (These can be changed subsequently.)

- CAN baud rate: 250 kbps
- Device ID: Identical to serial number (extended identifier format)
- V119: EM4100, Mifare, Hitag2 and Mifare AES are activated
- From V205: EM4100, Mifare, Hitag2 and NFC are activated
- Communication timeout: 30 seconds
(If there is no communication with the reader during this timeout, the LED flashes red).

8.2 Wiegand

HISAC® uses the 26-bit Wiegand format as standard. An alternative bit length can only be configured via the CAN bus.

The reader reads the UID of the card or tag used and transmits it including the leading and trailing parity bits. If a longer UID is used, this is limited according to the available bit length.

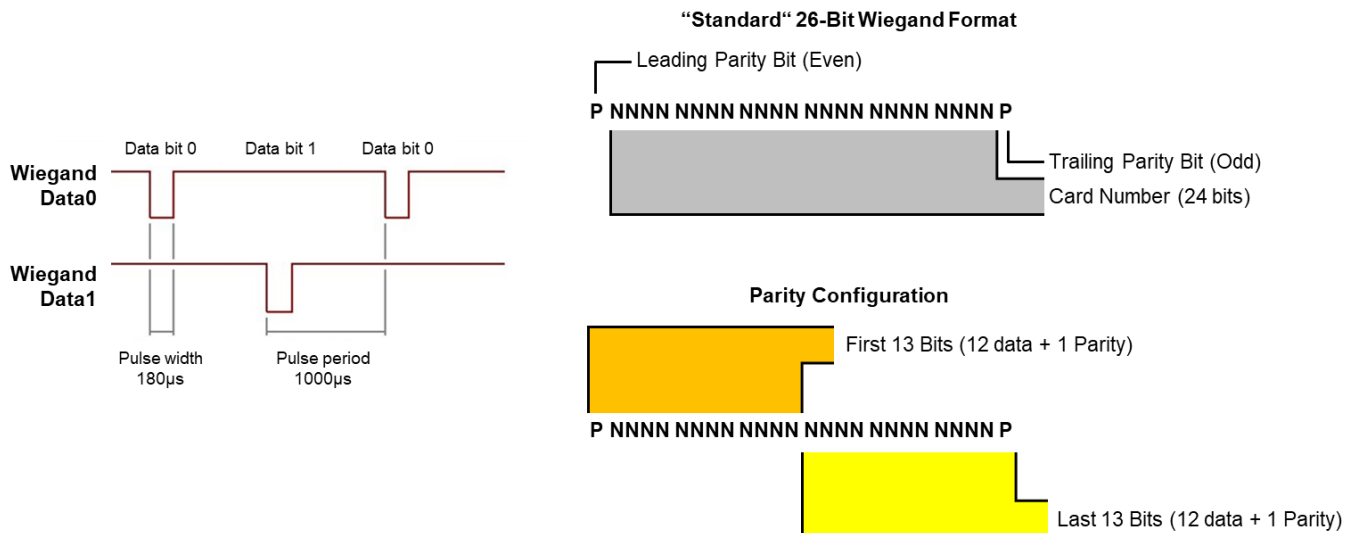


Figure 11: Wiegand protocol

To calculate the parity bits, the entire data area is divided into two halves. With an odd number of bits in Wiegand format, the middle bit is located at the interface of both halves and is therefore included in the calculation of both parity bits.



The AES master key, the AES application ID, the smartphone master key and the SID can only be parameterized via the CAN bus.

The reader does not have any internal pull-up resistors for the Wiegand signal lines Data0 and Data1. If the connected receiver device also does not have corresponding pull-ups, these must be added externally.



The maximum voltage of the Wiegand cables for the serial interface is 24V at a current of less than or equal to 5 mA. Higher voltages or currents can cause damage to the HISAC® and the bus system.

The following factory settings apply to this protocol:

- Wiegand format: 26-bit
- V119: EM4100, Mifare, Hitag2 and Mifare AES are activated
- From V205: EM4100, Mifare, Hitag2 and NFC are activated

9 Background information on DESFire AES support

The reader supports NXP DESFire cards and enables the retrieval of a 7-byte user ID from a specific file on the card. This function requires AES encryption and the correct configuration.

9.1 Configuration requirements

To activate AES support, the following parameters must be specified:

- A 16-bit application ID (AES Applications ID)
- A 16-byte AES encryption key (AES master key)

9.2 Behavior with activated AES

If AES encryption is activated, the Mifare UID of the card is no longer transmitted. Instead, the first 7 bytes of file number 0 are retrieved from the application ID and used as the user ID.

If one of the following conditions applies, no user ID is returned:

- The application is not available on the card.
- The specified AES encryption key is invalid.
- The specified file does not exist.
- The file size is smaller than 7 bytes.

9.3 Creating DESFire cards

An external card reader/writer and compatible software are required to create and configure DESFire cards. Make sure that the tool supports AES encryption and can configure file structures on the card.

9.4 Save AES Application ID and AES Masterkey on reader

The AES application ID and the associated AES master key must be stored in the reader. Further information on this can be found in the separate interface description under the *cmdSetDesfireApplication* and *cmdSetDesfireAESKey* commands or in the NFC documentation in the section on the test GUI.

Only if the application ID and the AES master key of the reader and the card match will the first 7 bytes of file number 0 be retrieved and returned as the user ID.

10 Background information on NFC support

In combination with the HISAC® app, the HISAC®-RFID-Reader supports authentication via smartphone. To do this, the access key provided by the key issuer must be imported into the app. Further information on the app and the integration and management of access keys can be found in the separate app and system integrator documentation.



NFC support is possible from firmware v205.

10.1 Preparation for HISAC® -RFID reader and enrollment

1. A **unique 64-bit SystemId SID** (8-byte ASCII) is defined once for the entire system (all HISAC®-RFID-Readers).
2. A **secret 128-bit master key MK** (16-byte ASCII) is created once for the entire system (all HISAC®-RFID-Readers).



Ensure that the master key (MK) is not made accessible to unauthorized persons under any circumstances. Protecting this key is crucial for the security of the entire system.

10.2 Smartphone preparation

Each participating smartphone installs the HISAC® app. When the app is started for the first time, the phone generates a random asymmetric key pair (RSA-Pub and RSA-Prv). The private key for decryption is stored in the phone's secure vault.

10.3 Enrollment

The end user presents their public key (RSA public key) to the key issuer. The enrollment system then generates an access key using a symmetric encryption method. This access key is made available to the end user and can then be imported into the HISAC® app on the smartphone. Only the smartphone that has the correct private key (RSA Private Key) is able to decrypt and use the access key.

As the access key contains both the master key (MK) and the system ID (SID), authentication can only take place on HISAC®-RFID-Readers that have been configured with the same MK and SID values. The master key and the SID must therefore be stored on the respective reader.

10.4 Authentication

1. The HISAC®-RFID-Reader presents itself as an NDEF tag with the URL "bss-sdi.com" as well as the **SID** and the random number **AUTH_CHALLENGE**.
2. The HISAC® app is registered to this URL and is started by the system.
Note: On iOS, the user must confirm each time the app is started. This is enforced by Apple and cannot be changed.
3. For each access key stored in the app with a matching **SID**, the **AUTH_CHALLENGE** is encrypted with **UPRV** and sent back to the HISAC®-RFID-Reader together with **UPUB** via NDEF Write.
4. Depending on the setting when the key is created, biometric user authentication is required (fingerprint, PIN or FaceID).

11 Procedure in the event of a malfunction

In the event of malfunctions, the following points must be checked:

Cabling:

- Are all cables switched correctly?

Control signals:

- Is the supply voltage of 12V DC or 24V DC applied?
- Are the required control signals (bus select) available on the HISAC®-RFID-Reader?
- Is the bus select signaled visually and acoustically during booting?

Installation:

- Is the housing damaged?
- Is the cable still firmly attached to the reader housing?

Operation:

- Does the LED light up correctly?
- Does the signal transmitter report?
- Are the cards or tags read?
- Are additional pull-up resistors necessary for Wiegand?
- Is the baud rate suitable for the cable length?