

Next level access since 1833

SAG



SAFE-O-TRONIC® access

Manual

Doorsystem

SAFE-O-TRONIC access®

DS

Information about this guide

© Copyright 2026 by Schulte-Schlagbaum AG

Navigeser Straße 100-110

D-42553 Velbert

Telefon +49 2051 2086-0

<http://www.sag-schlagbaum.com>

Edition: 20260417

Version: 3.11

Document number: 17.04.2026

This edition renders invalid all previous editions. Information in this document can be changed without prior announcement.



Note: Dissemination and duplication of this document, and use and disclosure of its contents, are prohibited unless expressly permitted. Violations will incur compensation for damage. All rights created by patent grant or registration of a utility model or design are reserved.

The information in this document has been compiled in good faith and to the best of our knowledge. Schulte-Schlagbaum AG extends no guarantee for the correctness or completeness of information in this document. In particular, Schulte-Schlagbaum AG cannot be held liable for consequential damage due to erroneous or incomplete information. Mistakes can never be prevented entirely despite all the effort taken, and so we appreciate when mistakes are pointed out to us.

SAFE-O-TRONIC® is a registered trademark of Schulte-Schlagbaum AG.

- This guide describes commissioning and operation of a *SAFE-O-TRONIC access®* device (see cover sheet for definition).
- The device may only be used for the purpose intended by the manufacturer.
- This guide must be kept in an easily accessible location.
- Unauthorised modifications and the use of spare parts and auxiliary devices that are not sold or recommended by the manufacturer may result in fire, electric shock and injury. Actions such as these result in exclusion of liability, and no warranty claims will be accepted by the manufacturer.
- Repairs may only be carried out by the manufacturer.
- The warranty provisions of the manufacturer as amended on the date of purchase apply to the device. Liability will not be assumed for inappropriate manual and automatic creation of parameters for a device or inappropriate use of a device.
- The operating company is responsible for setting up and connecting the device according to recognised technical regulations in the country of installation and other valid provisions.
- Screenshots are all taken in german versions of software - Position of the buttons are the same in other languages

Contents

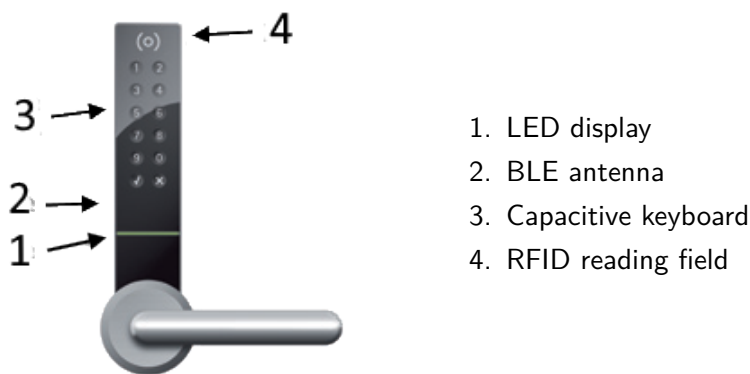
1	System overview	1
1.1	Intended use	1
1.1.1	Safety instructions	1
1.1.2	EU Declaration of Conformity	2
1.2	Controls	2
1.2.1	Bluetooth low energy (BLE)	3
1.2.2	Capacitive keyboard	3
1.2.3	RFID reading field	4
2	Installation and Commissioning	5
2.1	Installation	5
2.1.1	Preparation of the door	6
2.1.2	Mounting steps	6
2.1.3	Setting the handle direction	7
3	Commissioning	9
3.1	Test Functions	9
3.1.1	TestCode	9
3.1.2	TestKey	9
3.1.3	TestCommand	10
3.2	Programming	10
3.2.1	Series 200, 300, and 400	10
3.2.2	Series 500, 600, and 600 LEGIC	10
4	Operating Modes	11
4.1	PIN Entry	11
4.2	Fixed assignment	11
4.2.1	All-Open	11
4.2.2	TGC	12
5	Master Functions	13
5.1	Special features of the 200, 300, and 400 series	13
5.2	MasterKey	13
5.3	MasterCode	14
5.3.1	Entering the MasterCode	14
5.4	MasterCommand	14
5.4.1	Using MasterCommand	15

6	Data Structures	16
6.1	Explanations	16
6.1.1	Application	16
6.1.2	ID number	16
6.1.3	KGEN	16
6.1.4	Validity and schedules	16
6.1.5	Security PIN	17
6.1.6	Authorization via locking groups	17
6.1.7	Authorization via lock numbers	17
6.1.8	Authorization via areas	17
6.1.9	Blacklist	17
6.1.10	Data storage on transponder	17
6.2	Standard Generation 1	19
6.3	Standard Generation 2 - General	20
6.4	Fixed assignment - Locking groups	21
6.5	Fixed Assignment - Industry	22
7	Functions	23
7.1	PIN codes	23
7.1.1	Lockout due to incorrect entries	23
7.2	Time zone	23
7.3	Time functions	24
7.3.1	Valid from / to / from-to	24
7.3.2	Schedules - Standard	24
8	General Information	25
8.1	LED Display	25
8.1.1	LED display series 200, 300 and 400	25
8.1.2	LED display series 500, 600 and 600 LEGIC	28
8.2	Troubleshooting	36
8.3	Battery monitoring	36
8.3.1	Battery replacement	36
8.4	Maintenance and Care	37
8.5	Firmware Update	37
8.5.1	Updating Generation 1 Locks	37
8.5.2	Update for Generation 2 Locks	37
9	Technical Data	38
10	Technical information on batteries and battery packs	40
10.1	Series and battery life	40
10.1.1	LS	40
10.1.2	LSW	40
10.1.3	DS	41
10.1.4	CS	41

10.1.5 DSH	41
10.2 General information on battery life	41
10.2.1 Locking system variant	41
10.2.2 Transponder	41
10.2.3 Configuration and user behavior	42
10.2.4 Instructions for changing the battery	42
10.2.5 Disposal	42
List of Figures	43
List of Tables	44

1 System overview

Door locking systems from the *SAFE-O-TRONIC access*[®] DS series are mounted on the door leaf like a fitting. Locks from this series are equipped with various control elements. These can vary depending on the variant and activated components. This manual always assumes a DS in its full configuration. Test functions and programming options differ between the 200, 300, 400 series and the 500, 600, 600 LEGIC series.



Picture 1.1 – DS with all functions

⚠ Note: The appearance and range of functions may vary depending on the version ordered.

1.1 Intended use

The *SAFE-O-TRONIC access*[®] DS (DS) electronic door locking system is designed for installation in building doors and for locking and unlocking locks. The DS door locking system is only intended for use in protected indoor areas.

1.1.1 Safety instructions

- No modifications of any kind are permitted on Schulte-Schlagbaum AG (SAG) products, with the exception of those described in the relevant instructions.
- To avoid malfunctions and damage, only original parts and accessories may be used.
- The products must not be used to lock away emergency equipment that is vital in an emergency (e.g. defibrillators, emergency medication, and fire extinguishers).

- The products must not come into contact with paint or acids.
- Do not use products in potentially explosive areas.
- Only operate the products within the specified temperature range.
- Installation and battery replacement may only be carried out by trained personnel in accordance with the instructions.
- Only battery packs purchased from SAG may be used.
- Battery packs must not be charged, short-circuited, opened, or heated.
- Old or used battery packs must be disposed of properly.
- Keep battery packs out of the reach of children.
- The instructions should be passed on to the user by the person carrying out the installation.
- SAG accepts no liability for damage to the door or components caused by incorrect installation.
- No liability is accepted for incorrectly programmed units. SAG is not liable for any malfunctions, such as inability to access injured persons, property damage, or other damage.

 **Note: If a programmed lock is stolen from a system, this can compromise the security of the entire locking system. In such a case, please contact SAG to have your system reprogrammed and the security risk resolved.**

1.1.2 EU Declaration of Conformity

Schulte-Schlagbaum AG hereby declares that the device complies with the essential requirements and other relevant provisions of Directives 2014/53/EU and 2011/65/EU. The full version of the current CE Declaration of Conformity is available in English at:

www.sag-schlagbaum.com/news/eu-konformitaet/

1.2 Controls

Table 1.1 provides an overview of the control elements that are generally available in the respective lock variants. However, activation may depend on the license purchased.

The RFID function is only available to the operator for administrative purposes in the 200 series.

Table 1.1 – Overview of the various control elements

Lock variant	BLE	capacitive keyboard	RFID MIFARE	RFID LEGIC
200		×	[×	
300			×	
400		×	×	
500	×	×		
600	×	×	×	
600 LEGIC	×	×	×	×

1.2.1 Bluetooth low energy (BLE)

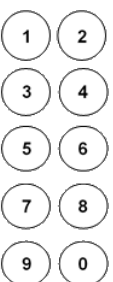
Locks in the 500, 600, and 600 LEGIC series all have a Bluetooth low energy interface (Bluetooth version 4.2). This can be accessed using SAG's own apps. The range of the BLE has been limited to approx. 3 m.

1.2.2 Capacitive keyboard

The capacitive keyboard has 12 or 13 keys, including 10 numeric keys and two or three additional function keys. The individual functions are listed in Table 2.1.

 **Note:** The capacitive keyboard cannot be operated with gloves on

Table 1.2 – Overview of the various capacitive keys

Button	Label	Function
	OK	Confirm code entry
	Cancel	Cancel code entry, all entries will be deleted
	Bluetooth	Activates the BLE interface for data transmission (only from series 500)
	Number keys	Enter a digit of a code

If there is a pause of more than three seconds between pressing the individual buttons, the entire entry

is canceled.

Otherwise, please note the information on PIN entry in chapter 7.1.

1.2.3 RFID reading field

The RFID reading field is located in the upper area of the lock. It includes the keys 1, 2, and Bluetooth. For the fastest and most reliable reading of the RFID data, the antenna overlap between the lock and the RFID transporter must be as large as possible. With coin transponders, this is best achieved by approaching the center. With card transponders, one corner of the card should be held in the reading field.



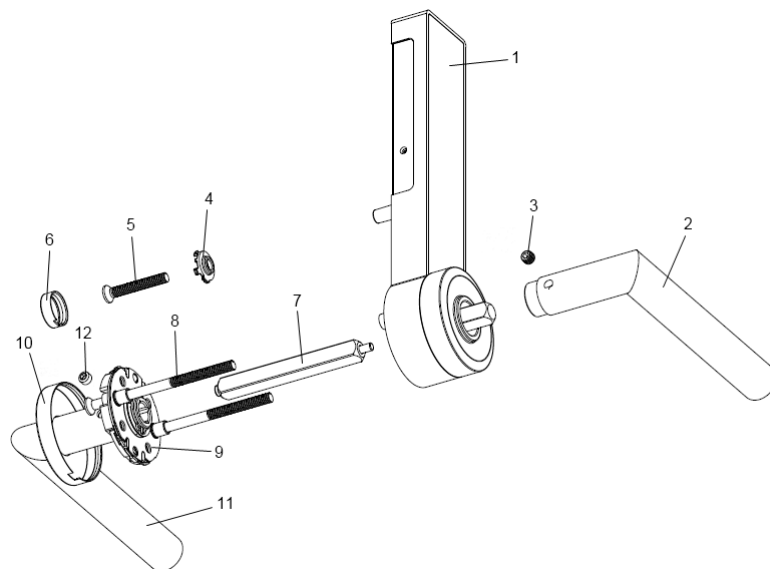
Picture 1.2 – DS with RFID reading field (red) and transponder card (green)

2 Installation and Commissioning

This chapter describes how to install the *SAFE-O-TRONIC access*[®] DS series locks on the door and the necessary preparations for the door.

⚠ Note: During installation and commissioning, the battery must be connected to the lock and the battery compartment closed. For instructions, please refer to chapter 8.3.1

2.1 Installation



Picture 2.1 – Installation of the lock

- 1 – Housing**
- 2 – Exterior door handle**
- 3 – Grub screw** for attaching the exterior handle
- 4 – Screw cover bracket** for the screw cover cap (6)
- 5 – Screw M5** for fastening the locking unit
- 6 – Screw cover cap** for covering the fastening screw (5)
- 7 – Square pin**
- 8 – Rosette screws** 2 pieces for fastening the rosette substructure
- 11 – Door handle, interior** with substructure of the rosette (9), handle rosette (10) and grub screw (12)

⚠ Note: The grub screws (ring-cut screws according to DIN 916 hard) of the handles must be tightened to a torque of 3 Nm. The screw lock is designed for single screw fastening.

⚠ Note: The rosette screws (8) must be tightened to a torque of 1.8 Nm to 2 Nm. The 2 Nm must not be exceeded.

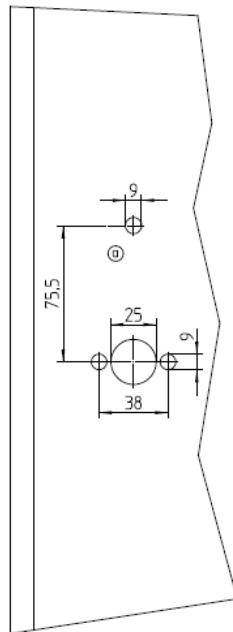
⚠ Note: The components screw (5), rosette screws (8) and square pin (7) depend on the door thickness and must be ordered according to the door thickness.

2.1.1 Preparation of the door

According to Picture 2.2, the following holes must be present in the door:

1. Hole measuring 25 mm and, for the rosette mounting, two holes with a diameter of 9 mm.
2. Hole with a diameter of 9 mm.

The holes can be drilled using a drilling template.



Picture 2.2 – Required holes in the door

2.1.2 Mounting steps

1. Prepare the door as described in chapter 2.1.1
2. Set the handle direction on the lock (see chapter 2.1.3)
3. Place the lock on the four holes 25 mm and 9 mm.
4. Insert the square pin (7).
5. Attach the sub-assembly rosette (9) with fixed door handle (11) to the door using two screws (8).

6. Screw the threaded pin (12) into the door handle (11), then slide the handle rosette (10) over the sub-assembly rosette (9).
7. Fasten the screw cover bracket (4) to the door with the screw (4). Then cover the screw (4) with the screw cover cap (6).
8. Fasten the door handle (2) with the threaded pin (3).
9. Test the function of the lock with the door open (see chapter 3.1).
10. Test the function with the door closed. Pay particular attention to the smooth operation of the latch and, in the version with internal locking, also to the smooth operation of the bolt.

2.1.3 Setting the handle direction

The *SAFE-O-TRONIC access*[®] DS door closing system can be used universally for different door directions. The handle direction is determined by an M3x10 stop screw. To do this, screw the stop screw into the right or left position.

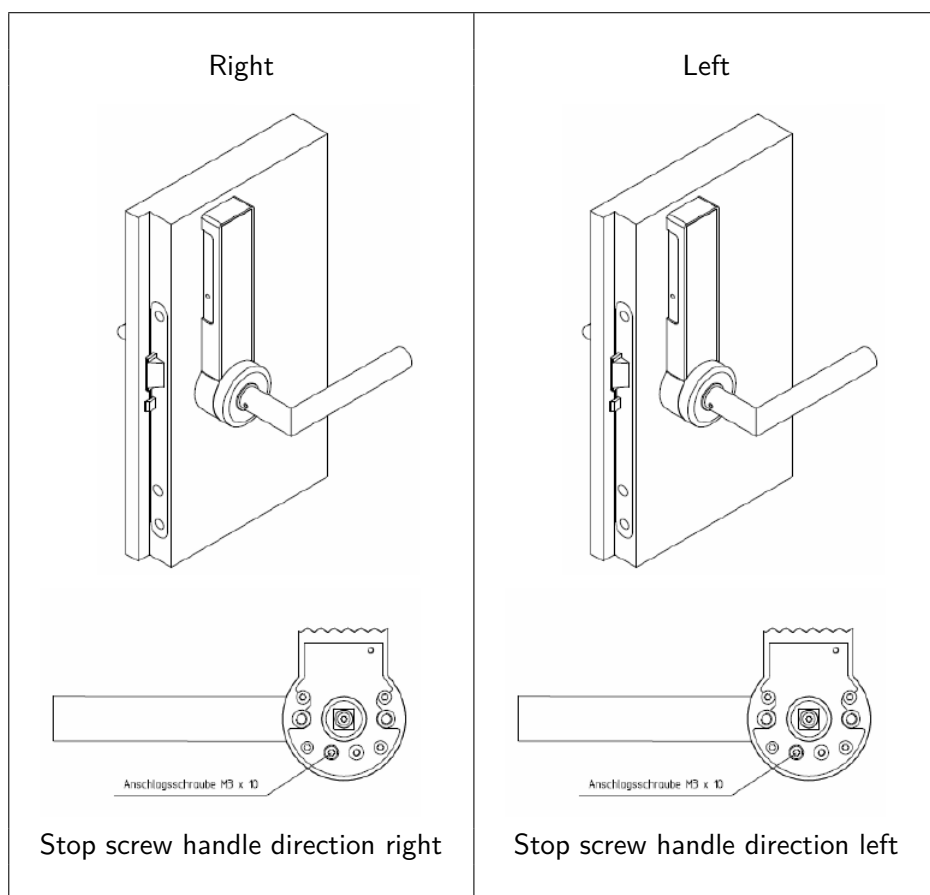


Note: Without the stop screw, the handle is not restricted from moving upwards from the neutral position.



Note: The handle direction must be set before installing the lock. An incorrect handle direction will lead to malfunctions.

Table 2.1 – Overview of the handle directions



3 Commissioning

Upon delivery, all locks are in factory condition. The TestCode (PIN), TestKey (RFID), and TestCommand (BLE) are also active. These are deactivated when the locks are programmed. To commission the locks of the *SAFE-O-TRONIC access*[®] DS series from series 500 onwards, *LockManager* (from version 7) or a separately available initialization file is required. The 200, 300, and 400 series can also be commissioned with *LockManager* version 6 or a ProgKey set. Programming is described in a separate manual.

3.1 Test Functions

The locks can be tested after installation using the test functions TestCode (PIN), TestKey (RFID transponder), and TestCommand (BLE command).

The test functions can only be used depending on the lock series. An overview can be found in the corresponding manual.

 **Note:** Particular attention must be paid to the smooth movement of the mechanical components when locking. A tight installation can lead to malfunctions.

 **Note:** All test functions remain active until the locks are programmed

3.1.1 TestCode

The test code consists of the buttons  and .

1.  Press button 0
2.  Press the OK button
3. Press the handle and check the latch movement

3.1.2 TestKey

Like any other transponder, the TestKey is held in front of the lock's reading field. The instructions in the manual must be followed. The lock is activated after the transponder has been successfully read.

After activation with the TestKey, the lock connects the handle to the mortise lock. The latch can be moved via the handle after release. The connection is disconnected again after a release time.



Note: Different test keys are required depending on the lock series and firmware version. Please contact the hotline if you have any questions.

3.1.3 TestCommand

To use the TestCommand, the SAG Management App (SAM) is required. Before the command can be transmitted, Bluetooth communication must be activated with the  button. This is necessary before each command transmission.

1. Activate Bluetooth as described in section ?? The blue LED flashes.
2. Select TestCommand in the SAG Management App (SAM) and send it.
3. Wait until the SAG Management App (SAM) has established the Bluetooth connection.
4. Press the handle and check the latch movement

3.2 Programming

Programming is described in a separate manual.

3.2.1 Series 200, 300, and 400

SAFE-O-TRONIC access[®] locks are programmed using the LockManager software (version 6 or higher) and the SystemKey set.

Alternatively, a ProgKey set can also be used for programming.

3.2.2 Series 500, 600, and 600 LEGIC

The *SAFE-O-TRONIC access*[®] locks are programmed using the LockManager software (version 7 or higher) and the Bluetooth SAG Management App (SAM).

Alternatively, a preconfigured initialization file can be used. These are available from SAG in certain configurations.

4 Operating Modes

The locks in the *SAFE-O-TRONIC access*[®] DS series can be used in different operating modes. All operating modes, with the exception of TGC mode, are available with all activation variants (PIN, RFID, BLE). The different activation variants are described in chapter 1.2. TGC always requires the PIN activation variant.

4.1 PIN Entry

1. Press buttons    
2.  Press the OK button
3. Press the handle

 **Note:** 2 4 3 5 is only an example code

 **Note:** The length of the user PIN can be changed in the lock settings in LockManager (4 to 6 digits)

 **Note:** Confirmation with the OK button is not necessary in some operating modes, or is only necessary when locking. In these operating modes, the lock is activated after the last digit has been entered.

4.2 Fixed assignment

For fixed assignment, the lock or transponder must be programmed with the user data authorized to lock. Fixed assignment can be used in different variants. These are described below.

4.2.1 All-Open

In All-Open mode, all user data known to the lock can operate the lock. It does not matter which user data the lock has used previously.

Example: User A locks the lock with their UserKey. User B opens the lock with their UserKey.

This operating mode is always useful when different users need to operate a lock. Examples include medicine cabinets in hospitals or door applications.

4.2.2 TGC

The TGC consists of two PIN codes. The first code is the StartCode. This code is 7 to 12 digits long and must always be entered by a user when using the lock for the first time. The code contains all the necessary information for the lock, such as the period of use. The second code is the ComfortCode. This code always has 4 digits and depends on the StartCode. The ComfortCode can be used after the StartCode has been entered for the first time, as long as it is valid.

TGC can be used from series 400 onwards.

5 Master Functions

This chapter describes the master functions for *SAFE-O-TRONIC access*[®] DS. Depending on the activated functions, individual functions may not be available. However, at least one master function is always available.

5.1 Special features of the 200, 300, and 400 series

The 200, 300, and 400 series distinguish between MasterKey 1 and 2. The same applies to the MasterCode. For better readability, only the MasterKey is described here; the behavior of the MasterCode is identical.

The MasterKey 1 is only used to open cabinets. It is not possible to lock cabinets with this key. Once opened, the lock remains locked and can no longer be used with a user medium. It can only be used again once the lock has been released by the MasterKey 2.

5.2 MasterKey

The MasterKey can be used at any time to operate a lock or release a lock.

A MasterKey must be programmed in the LockManager software before it can be used. The following parameters can be set:

1. Lock number or lock number range (local authorization)
2. Valid from, Valid until (time authorization)

This makes it possible to release the MasterKeys only for a specific lock or lock range and also for a specific period of time.

The last uses are stored on the MasterKey and can be read out using the LockManager software. This makes it possible to display the use of the MasterKey without reading out a lock log.

 **Note:** The MasterKeys can only be programmed in conjunction with the LockManager software. For locks in the 500, 600, and 600 LEGIC series, LockManager version 7 or higher is required. The other series can also be used with LockManager 6.

 **Note:** Every use of the MasterKey is stored in the lock log.

5.3 MasterCode

The MasterCode can be used at any time to operate a lock or release a lock.

The MasterCode has a minimum of 5 digits and a maximum of 9 digits. In addition, the MasterCode must always be at least one digit longer than the UserCode.

The MasterCode of a lock is stored in the application settings in the LockManager. It is always the same for an application (part of the entire system). The MasterCode remains unchanged until the lock programming is changed in the LockManager and the new programming is imported into the lock.

 **Note:** Each use of the MasterCode is stored in the lock log.

5.3.1 Entering the MasterCode

Press the buttons      

 **Note:** 3 5 1 9 7 is only an example code

 **Note:** Confirmation with the OK key is not necessary in some operating modes, or is only necessary when locking. In these operating modes, the lock is released after the last digit has been entered.

5.4 MasterCommand

The MasterCommand can be used at any time to activate a lock or release a lock.

A MasterCommand must be created in the LockManager software before use and transferred to the SAG Management App (SAM). The following parameters can be set:

1. Lock number or lock number range (local authorization)
2. Validity from, validity to (time-based authorization)

This makes it possible to generate MasterCommands only for a specific lock or lock range and also for a specific period of time.

The last ten uses of MasterCommands are stored in the SAG Management App (SAM) and can be displayed.

This makes it possible to display the use of the MasterCommand without reading a lock log.

 **Note:** The MasterCommands can only be programmed in conjunction with the LockManager software (version 7 or higher).

 **Note:** Each use of the MasterCommand is stored in the lock log.

5.4.1 Using MasterCommand

Activate Bluetooth as described in section ?? and wait for the visual confirmation (blue flashing LED). Then follow the instructions in the SAG Management App (SAM) .

6 Data Structures

A distinction is made between the data structures of Generation 1 locks (Series 200, 300, and 400) and Generation 2 locks (500, 600, and LEGIC). In Generation 1, only the standard data structure (see chapter 6.2) is available. In Generation 2, different data structures are supported depending on the firmware version. Optimizing the data structures and reducing them to the most necessary data guarantees optimal speed depending on the application. However, the selection of the data structure also results in a functional restriction, which must be taken into account when making the selection. The data structure used is defined for Generation 2 locks in the LockManager and transferred when programming the locks.

6.1 Explanations

The following terms are used to describe the data structures.

6.1.1 Application

An application is understood to be a locking area. This division is important because, for example, in free locker selection, the number of lockers that can be used simultaneously in an area can be limited. The number of applications is limited to eight for Generation 1 locks. For Generation 2 locks, there are only limitations due to the available storage space on transponders. If you have any questions, please contact the SAG hotline.

6.1.2 ID number

The ID number is a unique number for the key in the system. It is assigned by the LockManager.

6.1.3 KGEN

The KGEN (Key Generation) is the generation of the key. It is stored in the lock together with the ID number. The lock only accepts transponders with a KGEN equal to or greater than the last stored KGEN. Other transponders are rejected. The KGEN is updated by the transponder with the corresponding ID number.

6.1.4 Validity and schedules

Please refer to the chapter 7.3 for more information on this topic.

6.1.5 Security PIN

The security PIN is a two-factor authentication. The PIN must be entered on the lock before the transponder is held up to the lock. Access is only granted if the PIN entered matches the transponder data and the transponder is authorized.

6.1.6 Authorization via locking groups

Locking groups are virtual groups of locks. These groups can contain one or more locks. Each lock can be assigned to up to three groups in Generation 1 and up to five groups in Generation 2. A key stores the groups to which it is authorized.

A maximum of 500 locking groups can be assigned in each application. It is irrelevant whether there is a single lock or several locks in the group.

This type of authorization is particularly suitable for systems that have no more than 500 locks in one area and where one key must be able to operate many locks. An example of this is door locking systems in an industrial company.

6.1.7 Authorization via lock numbers

Lock numbers are unique numbers in a system. Up to 65,500 lock numbers can be assigned. Each lock has exactly one lock number.

With authorization via lock number, the unique lock number is stored in the key.

This type of authorization is particularly suitable for large systems in which a key is only authorized for a few locks. An example of this is changing room systems in an industrial company.

6.1.8 Authorization via areas

With authorization via areas, a lock number range is defined in which the key is authorized. The range is defined by a start and end lock number. For example, a key that is authorized for the range from 100 to 110 can also operate lock 105.

This type of authorization is particularly suitable for facilities in which an employee is responsible for defined areas. An example of this is cleaning staff in hotels.

6.1.9 Blacklist

The blacklist can be used to transfer KGEN / ID number combinations that are no longer authorized. The blacklist makes it possible to bring blocked KGENs into the locks via external transponders without having to go to each lock with the affected ID number.

6.1.10 Data storage on transponder

Various information is stored on the transponder, depending on the data structure. The data can be read out via the LockManager or a suitable terminal. All data is encrypted on the transponder.

The stored data includes the lock numbers of locks that have been locked with this transponder and battery information from the locks.



Note: Due to the limited storage space on the transponder, it is possible that not all locked locks are stored on the transponder. In addition, battery information is only available for the last locking action.

6.2 Standard Generation 1

Lock Generation	Min. Firmware	Speed	Remarks
1	1.0.0	medium	

Function	Support
ID number	Yes
KGEN	Yes
Schedules	Yes
Validity (from - to)	Yes
Security PIN	Yes
Authorization via locking groups	Yes
Authorization via lock numbers	No
Authorization via areas	No
Blacklist	No
Allows multiple locks in free locker selection	No
Usage duration (time span or point in time)	No
Action at the end of the usage duration	No
Lock battery status storage	Yes
Storage of locked locks	Yes

Description:

The Standard Generation 1 data structure is the only data structure supported in the 200, 300, and 400 series locks. It supports all data necessary for fixed assignment as well as free locker selection and is therefore not optimized for any specific application.

The Standard Generation 1 data structure operates at the sector level of a MIFARE Classic transponder. In this data structure, one application can be stored in a sector. Due to the limited storage space, only 128 locking groups are possible in a MIFARE Classic sector. In addition, an extended sector can be used, which increases the number of locking groups to 500. With other transponder technologies, all 500 locking groups are stored in one memory area.

6.3 Standard Generation 2 - General

Lock Generation	Min. Firmware	Speed	Remarks
2	1.6.1	slow	Obsolete - Data structure no longer supported from firmware version 2.9.1; Requires 2 memory areas

Function	Support
ID number	Yes
KGEN	Yes
Schedules	Yes
Validity (from - to)	Yes
Security PIN	Yes
Authorization via locking groups	Yes
Authorization via lock numbers	Yes
Authorization via areas	No
Blacklist	Yes
Allows multiple locks in free locker selection	Yes
Usage duration (time span or point in time)	Yes
Action at the end of the usage duration	Yes
Lock battery status storage	Yes
Storage of locked locks	Yes

Description:

The Standard Generation 2 - General data structure is the only data structure supported in the 500, 600, and LEGIC series locks up to firmware version 2.9.1. It supports all data necessary for fixed assignment as well as free locker selection and is therefore not optimized for any specific application. Due to the wide range of applications, read and write access to the transponder is slow. The transponder must therefore be held in the correct position for a long time (see chapter 1.2.3).

Two areas (start and application area) are required in the data structure.

6.4 Fixed assignment - Locking groups

Lock Generation	Min. Firmware	Speed	Remarks
2	3.4.1	medium	

Function	Support
ID number	Yes
KGEN	Yes
Schedules	Yes
Validity (from - to)	Yes
Security PIN	No
Authorization via locking groups	Yes
Authorization via lock numbers	No
Authorization via areas	No
Blacklist	No
Allows multiple locks in free locker selection	No
Usage duration (time span or point in time)	No
Action at the end of the usage duration	No
Lock battery status storage	Yes
Storage of locked locks	No

Description:

The Fixed Assignment - Locking Groups data structure is a data structure designed for fixed assignment, which is supported in the 500, 600, and LEGIC series locks from firmware version 3.4.1 onwards. The data structure can only be used for fixed assignment and is designed for this purpose.

The Fixed Assignment - Locking Groups data structure operates at the sector level of a MIFARE Classic transponder. In this data structure, one application can be stored in a sector. Due to the limited storage space, only 128 locking groups are possible in a MIFARE Classic sector. In addition, an Extended sector can be used, which increases the number of locking groups to 500.

With other transponder technologies, all 500 locking groups are stored in one memory area.

6.5 Fixed Assignment - Industry

Lock Generation	Min. Firmware	Speed	Remarks
2	3.4.1	medium	

Function	Support
ID number	Yes
KGEN	Yes
Schedules	Yes
Validity (from - to)	Yes
Security PIN	No
Authorization via locking groups	No
Authorization via lock numbers	Yes
Authorization via areas	No
Blacklist	No
Allows multiple locks in free locker selection	No
Usage duration (time span or point in time)	No
Action at the end of the usage duration	No
Lock battery status storage	Yes
Storage of locked locks	No

Description:

The Fixed Assignment - Industry data structure is a data structure designed for the fixed assignment of a small number of locks in a large facility, which is supported in the 500, 600, and LEGIC series locks from firmware 3.4.1 onwards.

The Fixed Assignment - Industry data structure operates at the sector level of a MIFARE Classic transponder. In this data structure, one application can be stored in a sector. In this data structure, the assignment on the transponder is carried out via the lock number. Due to the limited storage space, only 8 lock numbers are possible in a MIFARE Classic sector. In addition, an extended sector can be used, which increases the number of lock numbers that can be stored to 32.

With other transponder technologies, all 32 lock numbers are stored in one memory area.

7 Functions

The following chapter describes some of the lock's functions and their characteristics in more detail.

7.1 PIN codes

PIN codes can be entered on the lock using the capacitive keypad. PIN codes can be used in free (any PIN code with the set length) or fixed (PIN code is stored in the lock) assignment.

The following notes must be observed in all operating modes.

 **Note: PIN codes must be entered within 30 seconds. After this time, the previous entry is discarded.**

In a fixed assignment, the PIN codes must be programmed into the lock. Up to 100 PIN codes can be stored for Generation 1 locks and up to 400 PIN codes for Generation 2 locks. Fixed PIN codes support validity periods and schedules.

7.1.1 Lockout due to incorrect entries

If an unauthorized PIN code (e.g., a code other than the one used to lock the lock) is entered four times, the lock will lock for 60 seconds. During this time, no PIN codes will be accepted, even if the code entered is authorized. The only exception to this rule is the master code.

After 20 unauthorized entries, the lock will lock permanently. Only the master code will then be accepted. Entering the master code resets the lock and the lock can be used normally again.

 **Note: The locks are designed to prevent PIN codes from being guessed by trial and error.**

One-minute lock after four unauthorized entries

Permanent lock after 20 unauthorized entries

7.2 Time zone

The time zone setting determines the global time zone in which the lock is located. Among other things, this setting is used to correctly implement the summer/winter time changeover. Therefore, attention must be paid to this setting when commissioning the system.

 **Note: This setting is only available for Generation 2 locks. Generation 1 locks always use the settings for the Central European Standard Time time zone.**

7.3 Time functions

Locks in the *SAFE-O-TRONIC access*[®] DS series are equipped with a real-time clock that provides a variety of user functions. The time limits listed below are available as basic functions. Additional time limits can also be used. Outside the time limits, the lock cannot be operated and will not release. All time functions are available for all user data (PIN, RFID, and BLE). For RFID and BLE data, the restrictions can be stored on the corresponding media (RFID data carrier or BLE data). For PIN codes, the restrictions must be programmed into the lock.

 **Note:** When using time functions, make sure that the time in the lock is correct. An incorrect time can lead to unwanted actions or rejections, even during operation. For Generation 2 systems that use CLW, make sure that the time in the gateway is correct (NTP server according to RFC 5905 (NTPv4)). For more information, refer to the CLW documentation.

7.3.1 Valid from / to / from-to

These time limits specify from when, until when, or during what period the user data is valid. The restrictions can be made for a specific point in time (date and time). When restricting a period of time, two points in time (date and time) must be specified.

7.3.2 Schedules - Standard

In addition, 8 weekday-related time schedules can be programmed in the lock. This allows the validity of user data to be restricted to up to 8 different time periods (e.g., Mondays and Wednesdays between 8:30 a.m. and 4:20 p.m.). A maximum of 8 time schedules can be stored in each lock. The LockManager determines which schedules are active in the lock and how the individual schedule is defined. Each schedule contains the following values:

- Start of validity – minute, hour
- End of validity – minute, hour
- Valid weekdays – Mon, Tue, Wed, Thu, Fri, Sat, Sun, public holiday

A schedule in the lock is only valid if it has been activated. If a schedule is selected that is not active, the user data is valid without restriction.

 **Note:** Schedules can only be used with user keys (RFID) or user commands (BLE). They cannot be used with UserCodes (PIN) or TGC codes.

 **Note:** Schedules can also be used for night shifts with Generation 2 locks. In this case, the schedule begins on the selected days at the specified time and ends at the specified time on the following day.

8 General Information

8.1 LED Display

All important actions and operating states are indicated by the LED display and are intended to help identify the causes of malfunctions and operating errors. The meaning of the individual signals is explained in the following chapters.



Note:

-  means that the corresponding colored LED flashes.
-  means that the corresponding colored LED is active for the specified duration.

8.1.1 LED display series 200, 300 and 400



Picture 8.1 – Position of the various LEDs

Table 8.1 – Overview of the various LED status messages

green	red	green	red	Signal	Action
				Quick	programming mode
				Every 3 seconds	the lock time is active An incorrect code was entered four times
				1 second	button input
				1 second	Cancel button (X) pressed

green	red	green	red	Signal	Action
				3 times	Wrong handling - rotary knob was not pressed
				Alternating	operation possible
				1 second	Locking / programming successful
				2 second	Unlocking successful
				0,5 seconds	code was accepted
				3 seconds	internal malfunction
				First red then green	lock triggered by MasterKey 1 was released
				3 times fast	code entry denied - Lock by MasterKey 1
				3 times	battery warning
				5 times	battery empty
				3 times	reset performed

8.1.2 LED display series 500, 600 and 600 LEGIC



Picture 8.2 – Position of the various LEDs

Status messages version 1.x

Table 8.3 – Overview of the various LED status messages

blue	red	or- ange	green	Signal	Action
				3 times	reset performed
				permanent	initialization of memory
				1 time	key input
				8 times	PIN accepted
				1 time	cancel button pressed (X)
				1 time	cancel input
				Continuous	RFID processing
				1 second	programming successful
					reset in progress

blue	red	or- ange	green	Signal	Action
				6 times	battery warning
				10 times	battery empty
				every 500ms	actuation possible
				4 times	incorrect handling - rotary knob was not actuated
				500ms	locking / unlocking successful
				every 10s	locking time active (one minute) Rotary knob was not turned
				every second	Bluetooth active
				1 time	Bluetooth connection established
				1 time	Bluetooth data rejected
				1 time	Bluetooth terminated
				1, 5 seconds	internal malfunction
				1 second	FW update expected
				permanent	factory memory reset

Status messages version 2.x and 3.1.x

Table 8.5 – Overview of the various LED status messages

blue	red	or- ange	green	Signal	Action
				1 second	power on
				permanent	initialization of the memory
				5 seconds	restore settings
				permanent	RFID processing
				alternating every 50ms	motor drive
				alternating every 100ms (max. 2 seconds)	battery warning
				alternating every 100ms (max. 2 seconds)	battery empty
				alternating every 50ms (max. 2 seconds)	motor error
				max. 30 seconds	operation successful (or RFID removed)
				max. 30 seconds	rejected (or RFID removed)
				24ms	Bluetooth active
				1 second	programming successful

blue	red	or- ange	green	Signal	Action
				200ms	Bluetooth data rejected
				Every 3 seconds (10ms)	lock locked
				Every 3 seconds (10ms)	lock locked (MasterKey required)

Status messages from version 3.2.x on

Table 8.7 – Overview of the various LED status messages

blue	red	or- ange	green	Signal	Action
				Left to right	Power On
				Alternating every 200ms	Memory initialization
				Flashes every 200 ms	
				Flashes every 200 ms	Serious malfunction - contact the hotline
				Flashing	lock permanently blocked - Contact the hotline
				Flashing every 200ms	BLE active - connection possible
				Flashing every 200ms	BLE connection established
				Flashing every 200ms	
				Flashing twice	
				1 second	
				Flashing every 200 ms	

blue	red	or- ange	green	Signal	Action
				Flashing every 200 ms	Factory reset of the lock is being performed
				Flashing every 200 ms	Firmware update expected
				200 ms illumination	
				Flashing twice	Input canceled
				3 flashes	
				Flashing every 200 ms	RFID active and transponder being processed
				600ms	Data accepted
				2 flashes	
				3 flashes	
				Flashes every 200 ms	
				Flashing every 200 ms	Locking successful

blue	red	or- ange	green	Signal	Action
				Flashing every 200 ms	Unlocking successful
				flashing every 200 ms	
				Flashing every 5 seconds	
				Flashing every 200 ms	

8.2 Troubleshooting

The status messages on the LED display indicate errors and operating errors, which can then be rectified accordingly. If other, undefined states occur and the lock does not function properly despite replacing the battery and performing a reset using the reset command and reprogramming, please contact support.

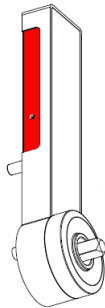
8.3 Battery monitoring

The automatic battery monitoring function of *SAFE-O-TRONIC access*[®] ensures that a lock with insufficient battery voltage can no longer be locked. The LEDs provide an advance warning of this. It is then advisable to replace the battery as soon as possible. The exact signaling can be found in chapter 8.1

If the battery is not replaced, an alarm will sound after a certain amount of time. This is indicated differently by the LEDs. The battery must now be replaced. In this state, the lock can only be opened, but no longer closed.

The locks may only be operated with batteries approved by Schulte-Schlagbaum AG. The use of non-approved batteries can lead to malfunctions and damage to the lock.

8.3.1 Battery replacement



Picture 8.3 – Replacing the battery

1. Loosen the screw on the side of the cover using a T6 screwdriver.
2. Open the battery compartment and remove the battery pack. Disconnect the two-pole plug connection of the battery pack. The plug must be pulled out straight, otherwise the connection box may be damaged. Connect the new battery pack to the plug connection and insert the battery into the lock using the battery replacement tool. Close the battery compartment and screw it back on.



Note: The battery must always be inserted with the pull tab facing the battery compartment cover.



Note: No code is deleted when the battery is replaced. To be on the safe side, the time should be reset after replacing the battery.



Note: The empty battery pack must be disposed of properly in accordance with the applicable environmental regulations!

8.4 Maintenance and Care

SAFE-O-TRONIC access[®] DS locks are maintenance-free. Under no circumstances may the locks be oiled or greased with mineral oil-based lubricants.

Cleaning may only be carried out with non-sticky, residue-free cleaning agents and disinfectants. No harsh cleaning agents, acids or alkalis may be used for maintenance. Pressure washers may also not be used. Hosing down the locks, e.g. with a hose, is also not permitted and may lead to damage and exclusion of liability.

8.5 Firmware Update

If available, SAG provides firmware updates. Updates typically include new features, bug fixes, or security updates.

When performing updates, a distinction is made between Generation 1 locks (Series 200, 300, and 400) and Generation 2 locks (500, 600, and LEGIC). All updates are performed individually on the locks.

 **Note: Updates must always be performed by SAG or at least under SAG's guidance.**

8.5.1 Updating Generation 1 Locks

Generation 1 locks are updated via a specially prepared Communicator (hardware provided by SAG) using the RFID interface. To do this, the lock must be in the programmed state and the Communicator must be configured for the corresponding system. To start the update, hold the Communicator up to the lock like an RFID transponder (follow the instructions in chapter ??). The green LED flashes while the transfer is in progress.

 **Note: The Communicator must not be removed from the lock during the transfer. The maximum distance allowed is 1 cm.**

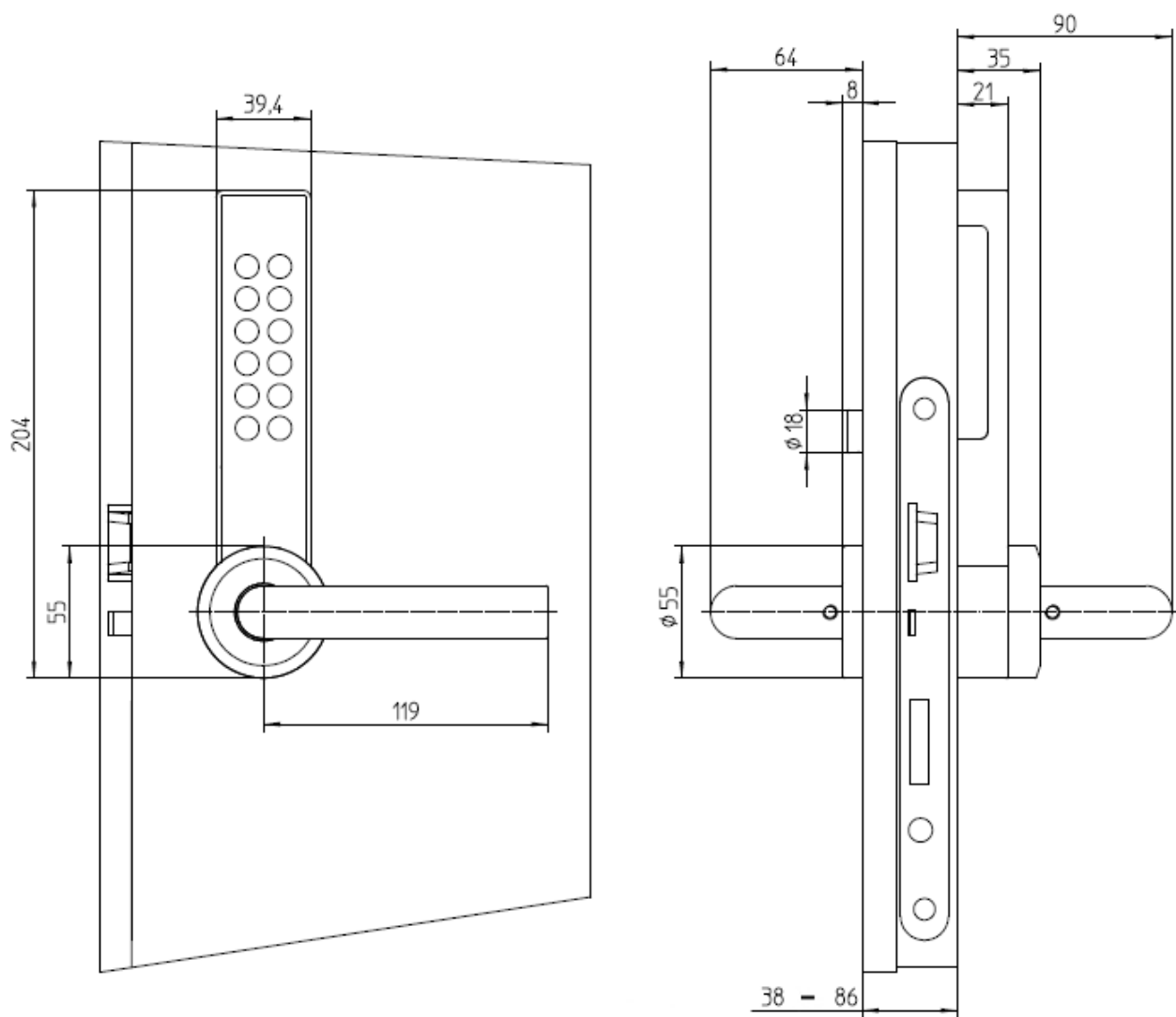
The lock confirms the transmission and the successful completion of the firmware update via the LEDs.

8.5.2 Update for Generation 2 Locks

Generation 2 locks are updated with new firmware via Bluetooth. To do this, the lock must first be put into update mode using a special Bluetooth command from the SAG Management App (SAM). For programmed locks, the command must match the system. The update is then transferred via a second app.

To perform a firmware update, please refer to the separate manual „Firmware Update via Bluetooth“ which you can obtain in its current version via the SAG hotline.

9 Technical Data



Picture 9.1 – Technical dimensions

Table 9.1 – Technical data

Display elements Series 200, 300, 400	2 x green LEDs; 2 x red LEDs
Display elements Series 500, 600, 600 LEGIC	1 x green LED; 1 x yellow LED; 1 x red LED; 1 x blue LED
Acoustic signal	signal generator
Battery	battery pack: 3 x alkaline cells (AAA)
Battery life* for Series 300	approx. 3 years or 30.000 actuations
Temperature range function	0 to +55°C
Temperature range storage	-15 to +55°C
Relative humidity	10 - 90 % non-condensing
Protection class	for protected indoor areas
RFID frequency	13.56 MHz
RFID transmission power	-11 dBm
BLE frequency (from series 500)	2.4 GHz
BLE transmission power (from series 500)	+3 dBm
Weight (without door handle)	approx. 600g
Housing dimensions (H x W x D)	204mm x 55mm x 21mm
Housing color	stainless steel
Bezel color	black or white
Door thickness	38 to 86mm



Note: Please note the information on battery life in chapter 10.

10 Technical information on batteries and battery packs

This chapter provides important information on battery life and the batteries used in *SAFE-O-TRONIC access*[®] locking systems.

The following temperature ranges apply to all locking systems:

Storage: -15 to +55°C

Alkaline battery function: 0 to +55°C

Lithium battery function: 0 to +55°C

Temperatures below 0°C lead to a limited battery life.

10.1 Series and battery life

The following batteries or battery packs are used in the *SAFE-O-TRONIC access*[®] locking systems.

 **Note:** The notes and restrictions listed in the 10.2 chapter must always be observed for the specified battery service life.

 **Note:** The specified battery life applies to the locking system variant 300

10.1.1 LS

Standard battery pack: Alkaline-manganese 3xLR03 (AAA)

Item number: # 38400200

Battery life* approx. 3 years or approx. 30.000 actuations

Special battery pack: Lithium 3xLR03 (AAA)

Item number: # 38400200L

Battery life* approx. 5 years or approx. 50.000 actuations

10.1.2 LSW

Standard battery pack: alkaline-manganese 3xLR06 (AA)

Item number: # 38450901

Battery life* offline approx. 4 years or approx. 55.000 Actuations

Battery life* online (radio status) approx. 3 years or approx. 30.000 actuations

Battery holder: for 3xLR03 (AA)

Item number: # 38450902

The batteries for the battery holder must be provided by the customer. Therefore, no statements can be made about battery life. Battery recommendation: alkaline manganese, Panasonic Powerline

10.1.3 DS

Standard battery pack: Alkaline-manganese 3xLR03 (AAA)

Item number: # 38400200

Battery life* approx. 3 years or approx. 30.000 actuations

Special battery pack: Lithium 3xLR03 (AAA)

Item number: # 38400200L

Battery life* approx. 5 years or approx. 50.000 actuations

10.1.4 CS

Standard battery: 2x lithium manganese dioxide CR-2L (3V)

Item number: # 50203EK-B

Battery life* approx. 3 years or approx. 30.000 actuations

10.1.5 DSH

Standard battery: 1x lithium manganese dioxide CR-2L (3V)

Item number: # 50203EK-B

Battery life* approx. 2 years or approx. 20.000 Actuations

10.2 General information on battery life

The battery life was determined under realistic laboratory conditions. This means that positive or negative deviations from these specifications are possible in practical use. The following list shows some properties and measures that can influence the battery life mentioned.

10.2.1 Locking system variant

The individual locking systems in the *SAFE-O-TRONIC access*[®] series differ in terms of their functionality and features. There are locking systems with PIN functionality (101 and 200), with RFID functionality (300), with a combination of PIN and RFID functionality (400), with a combination of PIN and BLE functionality (500) and with a combination of PIN, BLE and RFID functionality (600). The energy requirement for these locking systems varies and also influences the battery life. For example, the energy requirement for a 400 and 500 version is approx. 1.4 times higher than for the 300 version. The specified battery life refers to an average value that was determined with the 300 version.

10.2.2 Transponder

The energy requirement of the locking systems depends on the transponder type used. For example, the DesFire transponder in the Mifare transponder family requires the most energy for read or write access.

10.2.3 Configuration and user behavior

The configuration (release time, status display, etc.) and user behavior influence the battery life of the locking system. Details on this can be found in the corresponding chapters of the manuals.

10.2.4 Instructions for changing the battery

- The time at which the battery pack *SAFE-O-TRONIC access*[®] must be replaced depends on how often the locking system has been operated or how long the battery pack has been installed and on the ambient temperature in which the locking system is operated.
- Due to the low but unavoidable self-discharge of the batteries, it may be necessary to replace the battery pack before the specified number of actuations is reached.
- There is a risk of injury due to improper handling of the batteries.
- Only change the batteries when the door is open. A function check after a battery change should always be carried out with the door open.
- Installation and battery replacement should only be carried out by trained specialist personnel in accordance with these operating and installation instructions.
- Check the time after every battery change, the current time may need to be reprogrammed.
- Only use battery packs purchased from Schulte-Schlagbaum.
- Do not heat the battery above the specified storage temperature.
- Changing the CS300 battery: Avoid damage to the sealing ring due to improper handling. avoid. Do not use sharp objects and do not stretch the sealing ring more than necessary to push it on.
- Ensure correct polarity when inserting the batteries.
- Always replace discharged batteries with new batteries.
- Battery packs must not be recharged.

10.2.5 Disposal



Recycle defective or used battery packs in accordance with European Directive 2006/66/EC. Observe local regulations for separate disposal of batteries.

List of Figures

1.1	DS with all functions	1
1.2	DS with RFID reading field (red) and transponder card (green)	4
2.1	Installation of the lock	5
2.2	Required holes in the door	6
8.1	Position of the various LEDs	25
8.2	Position of the various LEDs	28
8.3	Replacing the battery	36
9.1	Technical dimensions	38

List of Tables

1.1	Overview of the various control elements	3
1.2	Overview of the various capacitive keys	3
2.1	Overview of the handle directions	8
8.1	Overview of the various LED status messages	25
8.3	Overview of the various LED status messages	28
8.5	Overview of the various LED status messages	31
8.7	Overview of the various LED status messages	33
9.1	Technical data	39