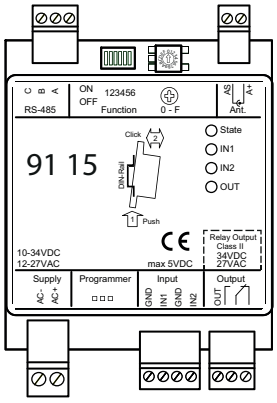


BEYOND SECURITY

Kaba Remote Reader 91 15-AM (US/CAN)

Technical Manual

- 06/2016

EN

Kaba AG
Access & Workforce Management
Hofwisenstrasse 24
8153 Rümlang
Switzerland

Phone +41 44 818 93 11
www.kaba.com

Kaba AG
Access & Workforce Management
Mühlebühlstrasse 23
8620 Wetzikon
Switzerland

Phone +41 44 931 61 11
www.kaba.com

Kaba GmbH
Access & Workforce Management
Albertistraße 3
78056 Villingen-Schwenningen
Germany

Phone +49 7720 603 0
www.kaba.com

This document must not be reproduced in any way or otherwise further used without the written consent of Kaba AG.
All product names are trademarks of the respective companies.

Copyright 2016 Kaba AG. All rights reserved.

- 06/2016

Contents

1 About this Document ... 7

1.1 Validity ... 7

1.2 Target group ... 7

1.3 Contents and purpose ... 7

1.4 Additional documentation ... 7

1.5 Change Log ... 9

1.6 Orientation in the document ... 9

1.7 Abbreviations/Term Definitions ... 9

1.8 Warnings ... 10

1.8.1 Hazard Categories ... 10

1.8.2 Symbols ... 10

1.9 Notes ... 10

2 Grouped safety messages ... 11

2.1 Use as directed ... 11

2.2 Mounting and Installation ... 11

2.3 Service and Maintenance ... 11

2.4 Accessories and spare parts ... 11

2.5 ESD (electrostatic discharge) protective measures ... 12

3 Product Description ... 13

3.1 Overview ... 13

3.2 Registration Unit Compatibility ... 14

3.3 Operating modes ... 15

3.4 Supported RFID Standards with Possible Media Definitions ... 15

3.4.1 MIFARE ... 15

3.4.2 LEGIC ... 16

3.5 Interface for Extension Modules ... 17

3.6 Technical Data ... 18

3.6.1 Overview of Technical Data ... 18

3.7 Conformity ... 20

3.8 Labeling ... 22

4 Design and function ... 23

4.1 Device variants ... 23

4.1.1 RFID reader ... 23

4.2 Device Structure ... 23

4.3 Firmware ... 24

4.4 System Connection ... 25

4.5 System Requirements ... 26

4.6 Behavior with Several Media in the Field (Anti-Collision) ... 26

4.7 Functions ... 26

4.8 Operating Modes ... 28

4.8.1 Overview of Operating Types ... 28

4.8.2 Online operation ... 28

4.8.3 Offline Operation ... 28
4.9 'Electric strike' operating mode ... 30
5 Installation ... 31
5.1 Installation conditions ... 31
5.1.1 General ... 31
5.1.2 Installation site ... 31
5.1.3 Connections ... 31
5.2 Installation layout (example) ... 32
5.3 Installation lines ... 33
5.3.1 Power supply line ... 33
5.3.2 Data line RS-485 ... 34
5.3.3 Line to the door opener and door contacts ... 39
5.3.4 Coaxial Cable to the Registration Units ... 39
5.3.5 Grounding Concept ... 40
5.4 Mounting the device and extension modules ... 41
5.5 Connections ... 43
5.5.1 Connections ... 43
5.5.2 Inputs IN1–IN2 ... 44
5.5.3 Output ... 46
5.6 Configuration ... 47
5.6.1 Directions for configuration ... 47
5.6.2 Switch ... 47
5.6.3 Set RS-485 termination resistances ... 48
5.6.4 Set peripheral address ... 50
5.6.5 Settings for “Electric strike” operating mode ... 51
5.6.6 Activate the monitoring of inputs ... 51
6 Start-up ... 52
6.1 "Standalone Access Control without Host System" Commissioning ... 52
6.1.1 Using LEGIC ... 52
6.1.2 Using MIFARE ... 53
6.2 Issue Write/Read Authorization (Launch) ... 54
6.3 Cancel Write/Read Authorization ... 54
6.3.1 Cancel all writing rights granted by a write authorization ... 55
6.3.2 Cancel a particular writing right granted by a write authorization: ... 55
7 Maintenance ... 56
7.1 Programming interface ... 56
7.2 Restart ... 56
7.3 Factory Reset/Reset Device to the Basic Status ... 57
7.4 Firmware Update/LEGIC OS Update ... 58
7.4.1 Firmware update/LEGIC OS update via access manager ... 58
7.4.2 Firmware Update / LEGIC OS Update with programmer 1460 ... 58
7.5 Updating configuration ... 60
7.6 Crossgrade ... 61
7.6.1 Device with Bxxx firmware (MRD) ... 61
7.6.2 Device with Axxx firmware (LEGIC) ... 61
7.6.3 Device with Mxxx firmware (MIFARE) ... 61
8 Troubleshooting ... 63
8.1 LED Displays on the Remote Reader ... 63

8.2 During Installation ... 63
8.3 During operation ... 64

9 Packaging/Return ... 66

10 Disposal ... 67
10.1 Decommissioning ... 67
10.2 Dismantling ... 67
10.3 Disposal ... 67

Index ... 68

1 About this Document

1.1 Validity

This document describes the product:

Product name:	Kaba Remote Reader 91 15 MRD Kaba Remote Reader 91 15 MIFARE Kaba Remote Reader 91 15 LEGIC
Functional type:	Access Manager
Date of manufacture:	April 2014 and later
Device software version:	RR 91 15-MRD = BRRB03.xxRx_ RR 91 15-M = MRRB03.xxRx_ RR 91 15-L = ARRB03.xxRx_

This document describes all device versions and optional equipment and functions. Options need to be paid for and are therefore only available if they have been purchased. Additional equipment and functions may not yet be available at the time of issuing the document and, possibly, can only be purchased at a later stage.

1.2 Target group

This document is exclusively intended for specialist personnel.

The descriptions require specialist personnel trained by the manufacturer. The descriptions do not replace product training.

For reasons of device safety, the installation and maintenance operations described in this document must be carried out only by service persons according to EN 60950-1 (Information technology equipment - Safety).

Service persons are persons having adequate technical training and sufficient experience to be aware of and to minimize the possible risks for themselves or other persons, which may occur when carrying out these operations. The service persons are responsible for adhering to the instructions given by the manufacturer and to the applicable standards and regulations during execution of their work.

This document is also used as information for persons with the following tasks:

- project planning and implementation
- Commissioning the product within the network
- Connecting the product to the user software by programming customer applications
- Customer-specific adjustment by setting the parameters of the product

1.3 Contents and purpose

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

1.4 Additional documentation

Supplementary documentation is available on the Kaba website. The technical manuals are located in a secured area of the website.

- Access is only possible after logging in.
- An account will need to be created before logging in for the first time.

Access and login:

1. In the browser, access the Kaba page http://www.kaba.com.
2. Select the language in the top right.

3. Under "Products", select the "Access Management" or "Workforce Management" product division.
4. In the top right section of the screen, click on the following symbol:
   .
5. Enter your e-mail address and password and login or create an account (see below).

⇨ The technical manuals can be found under "Downloads".

Create account:

1. Click "Create account".
2. Complete the data fields and confirm.
   ⇨ A confirmation link will be sent to your e-mail address.
3. To activate your account, click on the confirmation link in your e-mail.

1.5 Change Log

The most important changes to the last issue of this manual are listed below:

Version number	Edition	Brief description
TM_RemoteReader9115-AM-US-CAN_201606_en	06/2016	• First edition

1.6 Orientation in the document

This document contains the following orientation aids to facilitate finding of specific topics:

- The table of contents at the beginning of the manual gives an overview of all topics.
- The header always contains the respective main chapter.
- Cross references always indicate the number of the chapter in which the supplementary information can be found. Example [▸ 5.7].
- An index in the alphabetical order is given at the end of the manual.

1.7 Abbreviations/Term Definitions

Abbreviation/term	Description
Remote Reader	• Kaba Remote Reader 91 15
Device	• Kaba Compact Reader 91 10 AM
Registration unit	• Kaba Registration Unit 90 00 • Kaba Registration Unit 90 01 • Kaba Registration Unit 90 02
Host	• Host system
Control unit	• Kaba Access Manager
KCP	Kaba Communication Protocol (RS-485)
KMM	Kaba Media Manager
Access Manager	• Kaba Access Manager 92 00 MRD • Kaba Access Manager 92 00 LEGIC • Kaba Access Manager 92 00 MIFARE
Programmer	• Kaba Programmer 1460

1.8 Warnings

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

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

1.8.1 Hazard Categories

Warnings are split into the following categories:

⚠ CAUTION

Slight Risk

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

NOTICE

Information on how to handle the product correctly.

Failure to comply with these warnings may result in malfunctions. The product or something in its vicinity could be damaged.

1.8.2 Symbols

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

General danger

Danger for electronic components from electrostatic discharge

1.9 Notes

Notes are labeled with an info symbol.

Tips and useful information.
These help you to make best use of the product and its functions.

2 Grouped safety messages

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

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

2.1 Use as directed

The product is only intended for use as described in chapter “Product description”. Any use beyond that is considered contrary to its designated use. The manufacturer cannot be held liable for damage resulting from such use. Such use is at the sole risk of the user/operator.

2.2 Mounting and Installation

Mounting and installation may only be carried out by service persons (see chapter 1 “Target group”).

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

The manufacturer is not liable for damages resulting from improper handling or incorrect installation.

2.3 Service and Maintenance

Maintenance work / troubleshooting

Only the service person (see chapter 1 “Target group”) is entitled to remove faults and carry out maintenance work.

Reconstruction and modification

Any alteration or modification to the device may only be performed by the service person (see chapter 1 “Target group”). Any alteration or modification performed by unauthorized persons shall render void any liability.

2.4 Accessories and spare parts

Accessories and spare parts must comply with the technical requirements specified by the manufacturer. This is guaranteed when using original accessories and spare parts from Kaba.

2.5 ESD (electrostatic discharge) protective measures

NOTICE

Danger for electronic components due to electrostatic discharge.

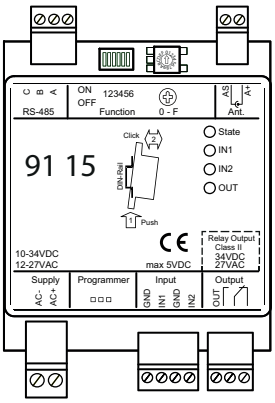
Improper handling of printed circuit boards or components can cause damages that lead to complete failures or sporadic errors.

- During installation and repair of the product, the ESD protective measures must be considered.
- Wear an ESD wristband when handling electronic components. Connect the end of the wristband to a discharge socket or an unvarnished grounded metal component. This way, static charges are discharged from your body securely and effectively.
- Touch only the edges of circuit boards. Do not touch the circuit board nor the connector.
- Place all dismantled components on an antistatic surface or in an antistatic container.
- Avoid contact between circuit boards and clothing. The wristband only protects the printed circuit boards against electrostatic discharge from your body, but there is still a risk of damage through electrostatic discharge from your clothing.
- Transport and dispatch dismantled modules only in electrostatically shielded protective bags.

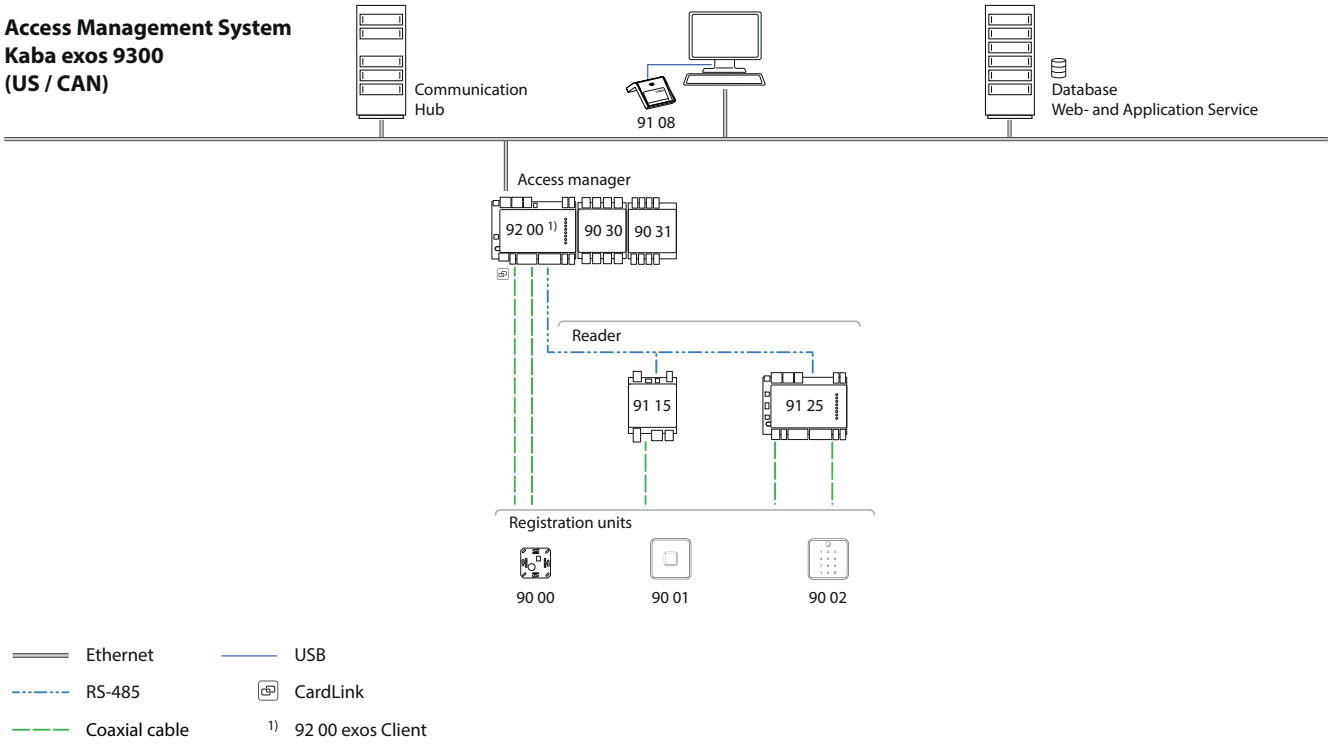
3 Product Description

3.1 Overview

The Kaba Remote Reader 91 15 with functional type AM can either control and monitor access control at access points or register coming/leaving bookings for time registration.



A registration unit can be connected to the Kaba Remote Reader 91 15.
Thanks to the separation of the remote reader and the registration unit, the remote reader can be installed in a tamper-proof area and the registration unit can be installed in an area that is not tamper-proof.
The remote reader can be integrated with the Kaba exos access control system.
The remote reader is installed on a DIN rail.
The door components (locking elements, monitoring contacts) are directly connected to the remote reader. This controls the electric strikes as well as the optical and acoustic signal transmitters of the registration units.
The remote reader communicates with the host system via the RS-485 interface. The host system checks the company codes and the user medium numbers, and activates the access points. If the communication between the remote reader and the host system is interrupted, then, with the relevant programming of its offline behavior, the remote reader automatically takes on the tasks of the host system; i.e. authorization checks and door functions are retained.



3.2 Registration Unit Compatibility

The following registration units are supported.

Registration unit	Control unit	
	Access Manager	Remote reader
		Functional type Access manager
Kaba registration unit 90 00	✓	✓
Kaba registration unit 90 01	✓	✓
Kaba registration unit 90 02	✓	✓

Registration unit	FCC	IC
Kaba registration unit 90 00	Tested Standard: FCC Code of Federal Regulations, CFR 47, Part 15, Sections 15.205, 15.207, 15.215 and 15.225	Tested Standard: Industry Canada Radio Standards Specifications RSS-GEN Issue 4, Sections 8.8, 8.9 and 8.10 and RSS-210 Issue 8, Section A2.6 (Category I Equipment)
Kone registration unit PCB		
Kaba registration unit 90 01		
Kone registration unit 90 01		
Kaba registration unit 90 02		
Kone registration unit 90 02		

3.3 Operating modes

The door configuration determines the operating mode of the device. A detailed description of the door configurations and their operating modes can be found in the chapter 'Electric strike' operating mode [▸ 4.9].

3.4 Supported RFID Standards with Possible Media Definitions

The following table shows the RFID standards and media definitions supported by the device.

The Kaba Remote Reader 91 15 recognizes up to eight different media definitions at the same time.

Media definitions		**Supported RFID technologies**				
		MIFARE DESFire	**MIFARE Classic**	**LEGIC advant**		**LEGIC prime**
		ISO 14443A	**ISO 14443A**	**ISO 14443A**	**ISO 15693**	**LEGIC RF**
Unique number (UID) *1		✓	✓	✓	✓	-
Safe UID		-	-	-	-	✓
Card ID		✓	✓	✓	✓	-
Kaba group header		-	-	✓	✓	✓
Kaba advant ID		-	-	✓	✓	-
LEGIC access™ (advant)		-	-	✓	✓	-
LEGIC access™ pool (prime)		-	-	-	-	✓
CardLink 1.1	Data	✓	✓	✓	✓	-
	Actuator status	✓	✓	✓	✓	-
	Media traceback *2	✓	-	✓	-	-
CardLink 1.0	Data incl. actuator status	-	-	-	-	✓
Additional media numbers		✓	✓	✓	✓	✓
*1		The LEGIC chip set does not use the safe UID command set so that UID from other media, such as MIFARE, can also be read.				
*2		Media traceback information can only be read out directly on the access manager and no media traceback information is written.				

3.4.1 MIFARE

The system can evaluate everything that can be defined in Kaba media manager. MIFARE DESFire or MIFARE Classic media can be read and described on the same Kaba Remote Reader 91 15 MIFARE using various media applications.

3.4.2 LEGIC

LEGIC prime or LEGIC advant media can be read and described on the same Kaba Remote Reader 91 15 LEGIC using various media applications (LEGIC advant media can only be described using LEGIC advant components).

Dual chip card

A dual chip card with LEGIC advant (14443 A) and CardLink LEGIC prime (LEGIC RF) is supported.

3.5 Interface for Extension Modules

The extension modules are connected to the system bus of the Kaba Remote Reader 91 15. There is a limit to the maximum number of supported extension modules. The host system determines the maximum number of connectible extension modules.

A maximum of 2 extension module 90 31 (8 inputs) and 2 extension modules 90 30 (8 relay outputs) can be plugged in via the serial port on this interface.

3.6 Technical Data

3.6.1 Overview of Technical Data

Mechanics	
Mounting	• Installation location: see • On DIN rail in accordance with EN 50022
Housing	• ABS black, with imprinted connection diagram
Combustion category	• HB (UL94)
Dimensions	• 70 x 106 x 45 mm (L x W x H) or four space units of 17.5 mm width measurement including screw/plug terminals
Connections	• All connections are screw/plug terminals • Max. relay load: 2 A

Power supply	
Input voltage, without external wiring	• 12–27 V AC (50/60 Hz) or 10–34 V DC • Power consumption/thermal output: max. 5 W
The device may only be supplied with SELV (Safety Extra Low Voltage) and LPS (Limited Power Source), according to IEC/UL/CSA 60950-1.	
Clock	• The clock can run for at least 120 hours without a power supply (after at least 10 minutes in operation)

Interfaces	
HF RFID	• 1 registration unit with or without keypads • Coaxial cable, impedance 50 Ohm • Encrypted data transfer • See also 3.4
RS-485	• To connect to the host control unit • KCP protocol; galvanically isolated, 2-wire • Baud rate 19200 baud • 8 data bits, even (Even) parity, 1 stop bit • Termination resistance for bus or star wiring • Addressing 1–8
Programmer interface	• For firmware update or programmer connection
Extension modules	• Maximum number of supported extension modules, see chapter 3.5

Inputs and outputs	
2 binary inputs	• With internal power supply and common ground, for connection of insulated switches • Maximum 5 V DC • Line monitoring (can be disabled) • LED status indicator
1 relay output	• Switch contact: max. 30 V DC/AC max. power 2 A • Switching cycles at 30 V DC/1 A typical 500,000 (VdS 2358 requirement is 200,000) • Switching cycles at 30 V DC/2 A typical 100,000 • LED status indicator

Ambient conditions	
Ambient conditions	• Operating temperature: -25 °C to +70 °C • Storage temperature: -40 °C to +85 °C • Relative humidity: 0% to 95%, non-condensing • Protection class as per IEC 60529: IP20

Also see about this

3.4 Supported RFID Standards with Possible Media Definitions [▸ 15]

5.1.2 Installation site [▸ 31]

3.7 Conformity

This product conforms to the following standards:

EN 60950-1:2006/A2:2013
UL 60950-1:2007/R:2014-10
CAN/CSA-C22.2 No. 60950-1:2007/A2:2014-10

EN 301 489-1 V1.8.1:2008
EN 301 489-3 V1.4.1:2002

EN 300 330-1 V1.7.1:2010
EN 300 330-2 V1.5.1:2010

in accordance with the provisions of the EC directives

2006/95/EC Low voltage directive
1999/5/EC R&TTE directive
2004/108/EC EMC directive

RoHS This device complies with the regulations of the Directive **2011/65/EU** of the European Parliament and of the Council of June 8, 2011, on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

The original Declaration of Conformity can be downloaded from **www.kaba.com/conformity** in PDF format.

Tested Standard:

FCC Code of Federal Regulations, CFR 47, Part 15, Sections 15.205, 15.207, 15.215 and 15.225

FCC ID NVI-KRR9115-K5

FCC § 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.

FCC § 15.21 (Warning Statement)

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

FCC § 15.105

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Tested Standard:

Industry Canada Radio Standards Specifications RSS-GEN Issue 4, Sections 8.8, 8.9 and 8.10 and RSS-210 Issue 8, Section A2.6 (Category I Equipment)

IC:11038A-KRR9115K5

ICES-003

This Class A digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Canada RSS-GEN 8.4

This device complies with Industry Canada's licence-exempt RSSs. 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; 2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

3.8 Labeling

The identification plate is located on the side of the device.

The following information can be found on the identification plate:

- Device designation
- Article number
- Serial number
- Function type
- Connection data (power supply)
- CE mark
- WEEE mark as per DIN EN 50419

4 Design and function

4.1 Device variants

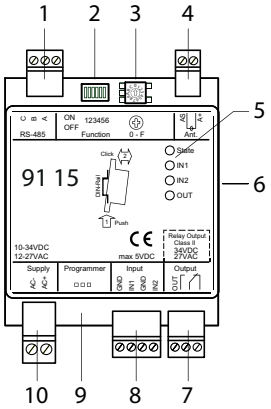
4.1.1 RFID reader

Kaba Remote Reader 91 15 is available in the following RFID reader variants:

- MIFARE
- LEGIC

The host system determines which RFID media technology (MIFARE or LEGIC) the Compact Reader supports.

4.2 Device Structure



1 RS-485 interface

2 Function

3 Rotary switch (addressing)

4 Antenna

5 LED Displays

6 Interface for Extension Modules

7 Relay output OUT

8 Inputs IN1–IN2

9 Interface for Kaba programmer 1460

10 Power supply

4.3 Firmware

The hardware of this product is used in various Kaba system solutions. The functions and possible uses of the product are determined by the firmware used.

This manual exclusively describes the Kaba Remote Reader 91 15 with functional type Access Manager (AM).

Firmware designation

Reader type	**M**	MIFARE
	A	LEGIC
	B	MRD (multi RFID device) LEGIC or MIFARE (determined during commissioning)
Device type	**RC**	Compact reader
	RR	Remote reader 91 15
	RE	Remote reader 91 25
Functional type	**A**	E300 V4 or N300/T300/U300 V3
	B	Access Manager
	C	Subterminal
	E	AMC/II (cDML)
Version number	**xx.xx**	Version
Addition 1	**R**	Final, approved version
Addition 2	**A**	Subversion
Addition 3	_	Reserve

Example

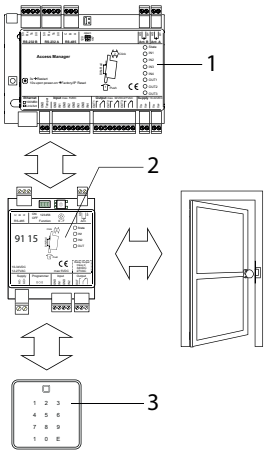
Designation of firmware for Kaba Remote Reader 91 15 with functional type Access Manager:

- BREB03.xxRxx (MRD)

Firmware mark on the product

Devices with firmware with the functional type access manager bear a mark reading "Type: Access manager" on the identification plate.

4.4 System Connection



The Remote reader communicates with the host control unit via the RS-485 interface.

Functions of the host control unit (1)

- Checking access data received by the Remote reader
- Authorization check
- Sending commands for optical and acoustic user guidance to the Remote reader
- Sending commands for relay control to the Remote reader

Functions of the remote reader (2)

See Overview [▸ 3.1]

Functions of the registration unit (3)

- Reading the media held up (RFID)
- Optical and acoustic user guidance
- Keypad for PIN entry and additional functions with numeric codes

Behavior in the event of an interruption in communication

In the event of an interruption in communication, the Remote reader automatically takes over some of the tasks of the host control unit. A simplified authorization check and simplified door functions remain available. The parameterization determines off-line behavior.

4.5 System Requirements

Host control unit

- Kaba access manager 92 00 MRD
- Kaba access manager 92 00 LEGIC (for Remote readerLEGIC)
- Kaba access manager 92 00 MIFARE (for Remote reader MIFARE)

System software

- Kaba exos 9300

4.6 Behavior with Several Media in the Field (Anti-Collision)

The device (Kaba Remote Reader 91 15) can recognize several LEGIC advant user media (ISO 14443 A) in the field simultaneously. Only the first user medium that corresponds to the search criteria defined in the system is considered. The remaining user media are ignored.

4.7 Functions

All data for access decisions are saved in the host control device. The authorization check of a badge and access control are undertaken by the control device.

Functions available before connection to the host system

Standalone access control (without host system); see chapter "Standalone Access Control without Host System" Commissioning

Access control functions

- Authorization check using badges and temporal authorization including verification
- Connection of a remote registration unit
- Control of optical and acoustic signal transmitters of the registration unit
- Control of electric strikes (doors with electrical blocking elements)
- Support for a connected door release button or door handle contact
- Monitoring of the door status with frame contact, bolt monitoring and door handle contact
- CardLink support: Validating and Invalidating
- CardLink support: Validation and UID additional recording (LEGIC only)
- Hold-open mode, so that, when access is authorized, the door remains open for as long as the badge remains within range of the antenna (field)

Restrictions with interrupted connection (offline)

MIFARE

Reduced authorization check using site keys.

Door function is retained depending on the offline parameter setting, see Switch [▸ 5.6.2].

- Authorization check using site keys. A maximum of eight site keys can be saved.
- Not taken into consideration: Time Zones
- Logbook for 2000 events
- No room monitoring/balancing and no CardLink functionality
- No change in fabrication key

LEGIC

Reduced authorization check using segment search keys. Door function is retained depending on the offline parameter setting, see Switch [▸ 5.6.2].

- Authorization check using segment search keys. A maximum of eight segment search keys can be saved.
- Not taken into consideration: Time Zones
- Logbook for 2000 events
- No room monitoring/balancing and no CardLink functionality

Restored connection

Automatic forwarding of saved bookings as well as status and alarm messages when connection is restored.

4.8 Operating Modes

4.8.1 Overview of Operating Types

The device supports online and offline operating modes.

Online operation: The device communicates with the system.
See Supported functions

Offline operation: If a device connected with the system is disconnected from the system, then it switches to offline mode.
See Supported functions

For the online and offline operation of the device, a minimum of the following hardware settings must be carried out before putting into operation:

System used	Minimum hardware settings
Kaba exos 9300	**Online operation:** • Address **Offline operation:** • DIP and rotary switch

4.8.2 Online operation

In online operation, the Remote reader communicates with the host system. The system makes the access decision on the basis of badges, time-dependent authorization and verification. The system controls the access points. If communication between Remote reader and system is interrupted, then the Remote reader independently switches into offline operation. If the Remote reader is queried by the system again, then the Remote reader switches back into online operation.

4.8.3 Offline Operation

Even in offline operation, i.e. without communication with the host system, an access point is monitored and controlled by the Remote reader. For access decisions,
site keys are used under **MIFARE** and
segment search keys are used under **LEGIC**.
The Remote reader controls the access point according to the position of the DIP switch.
In order to ensure fault-free offline operation, the Remote reader should be operated with a secure power supply (e.g. UPS).

Behavior in the event of an interruption to communication

- The access point goes to basic status (possibly alarm, if the access point is not closed)
- Relays which are not involved in a door process (according to DIP switch) deactivate; the same is true for the connected Kaba extension module 90 30

4.8.3.1 Offline Access Decision

The customer determines the nature of the offline access decision which is parameterized in the system. We differentiate the following offline access decisions:

Parameter settings in the system: no offline access decision

The Remote reader rejects all bookings in offline operation.

Parameter settings in the system:
Checking site key (MIFARE)/segment search key (LEGIC)

In the online mode, the site key (MIFARE)/segment search key (LEGIC) is sent to the Remote reader by the system and saved in the Remote reader. During the offline mode, the Remote reader only checks the site key (MIFARE)/segment search key (LEGIC). The time zone is not considered for this kind of access decision.

Logbook

The logbook records and saves a maximum of 2000 events during the offline operation. Once the Remote reader is online again, the saved data is sent to the host system and deleted from the memory of the Remote reader.

The following events are logged:

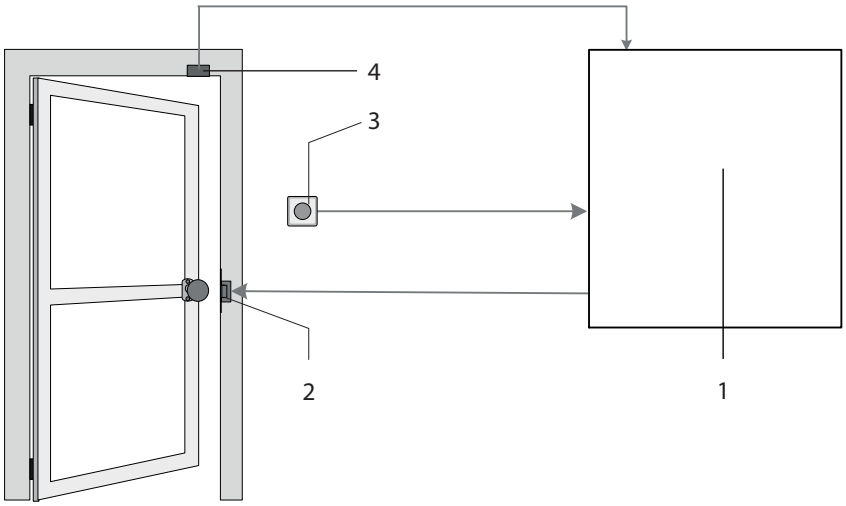
- Authorized accesses (incl. type of authorization)
- Tampering, door forced open, door opener key

If there are more than 2000 entries, the oldest will be overwritten (ring memory).

Service mode

See chapter Service mode

4.9 'Electric strike' operating mode



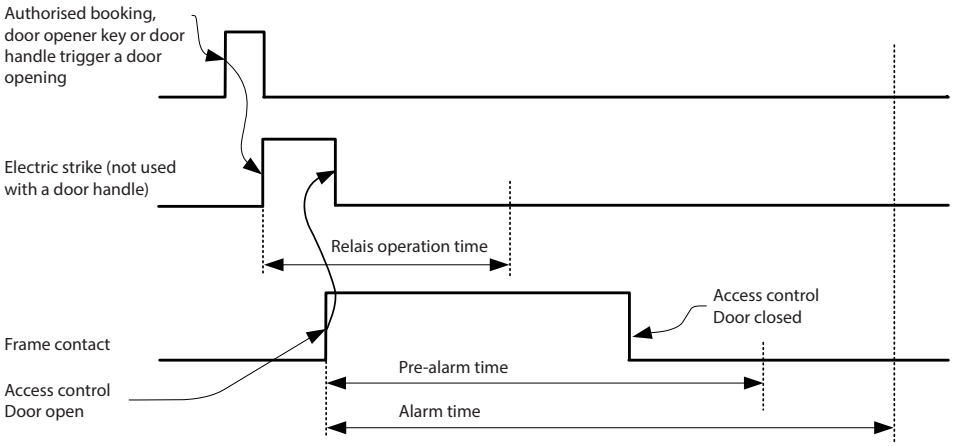
1 Kaba Remote Reader 91 15

2 Electric strike

3 Door opener key

4 Frame contact (Access control)

In ‘Electric Strike' operating mode, primarily doors with electrical blocking elements (door opener, magnet) are operated.
The electric strike is actuated when triggered by an authorized booking or the door opener key. The door is now released for opening and the set relay operation time starts to run. When opening the door, the pre-alarm and alarm time start to run ('Door open too long').



5 Installation

5.1 Installation conditions

5.1.1 General

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

5.1.2 Installation site

The device is assembled on a DIN rail in a housing or IT cabinet.

The device should be installed in a tamper-proof location within the area to be secured.

Electromagnetic fields

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

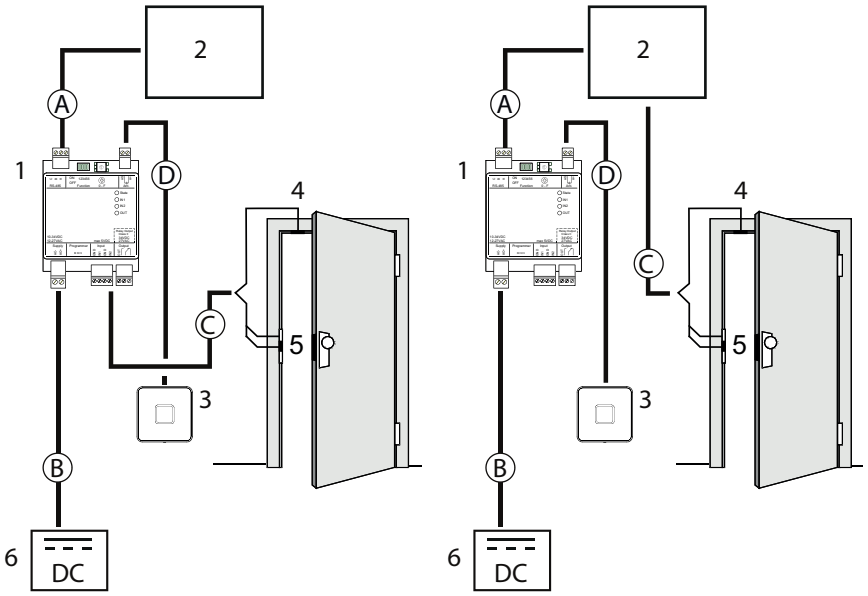
5.1.3 Connections

The following connections must be available at the location where the access manager is to be installed:

- Power supply for the device
- RS-485 cable to the host device
- Cables to door openers and switches
- Coaxial cable to registration units

The installation lines have to be flush with the surface or be laid in the vandal-proof area.

5.2 Installation layout (example)



1 Kaba Remote Reader 91 15
2 Kaba access manager 92 00
3 Kaba registration unit
4 Door frame contact
5 Door contact, door opener
6 Power supply

Installation cables

A Data line
B Power supply line
C Line to the door opener and door contacts (if required)
D Coaxial cable

5.3 Installation lines

5.3.1 Power supply line

Power can be supplied in the following ways:

- From the host control device (power supply and data line in one cable)
- From a separate power supply

NOTICE

Voltage drops, caused by line resistance, must be taken into consideration for long lines.
The given cable types and diameters are examples and serve as recommendations. The technical specifications of the cable manufacturer are authoritative for the precise determination of the cable diameter/cross section and the resulting maximum cable lengths. The voltage drop across the cable length is decisive in this case. As such, the voltage that is available at the end of the cable may, under no circumstances, be less than the minimum permitted supply voltage of the connected components. This always applies in consideration of the maximum power consumption of the connected components.

Only connect the terminals when the power is switched off.

Notice: The device may only be supplied with SELV (Safety Extra Low Voltage) and LPS (Limited Power Source), according to IEC/UL/CSA 60950-1.

5.3.1.1 Power supply from the host control device

(Central power supply)

Power is supplied from the host control device.

In the case of bus wiring, the power supply and data line can be carried in one cable (maximum total length of 350 m).

In the case of star wiring, the power supply and data line can be carried in one cable (maximum length per stub of 20 m).

A separate power supply must be used for greater distances.

Permissible Cable Lengths and Cable Types				
Type of wiring:	**Star**	**Bus**		
Max. cable length:	**< 20 m** (per stub)	**< 50 m** (total)	**< 100 m** (total)	**< 350 m** (total)
Cable type CAT.5 S-UTP *	4 x 2 x AWG 24		4 x 2 x AWG 22	4 x 2 x AWG 20
Cable type J-Y (ST)	4 x 2 x ø 0.6 mm		4 x 2 x ø 0.8 mm	4 x 2 x ø 1.0 mm

*S-UTP (screened unshielded twisted pair)

Do not ground the compact reader/remote reader.

5.3.1.2 Power supply and data transfer in separate cables

(Local power supply)

Data lines and power supply lines are carried with one of each in a cable.

Power is supplied locally, e.g. from a power supply unit.

A local power supply can be used in the following cases:

- in long data lines
- if there are increased requirements regarding the operational safety of the device (offline capability).

Permissible Cable Lengths and Cable Types				
	Data line RS-485			**Power supply**
Type of wiring:	**Star**	**Bus**		
Max. cable length:	**< 100 m** (per stub)	**< 1200 m** (total)		**< 10 m**
Cable type CAT.5 S-UTP *	2 x 2 x AWG 24			1 x 2 x AWG 24
Cable type J-Y (ST)	2 x 2 x ø 0.6 mm			1 x 2 x ø 0.6 mm

*S-UTP (screened unshielded twisted pair)

Notice: The device may only be supplied with SELV (Safety Extra Low Voltage) and LPS (Limited Power Source), according to IEC/UL/CSA 60950-1.

5.3.2 Data line RS-485

Only connect the terminals when the power is switched off.

The device is connected to the host control device via a two-wire party line connection (RS-485).

For information on permissible cable lengths and cable types, please see:

- Power supply from the host control device [▸ 5.3.1.1]
- Power supply and data transfer in separate cables [▸ 5.3.1.2]

5.3.2.1 Cable

NOTICE

Local legal provisions (e.g., VDE) must be observed during installation of components.
For notes on structured cabling, see the standard EN 50173.

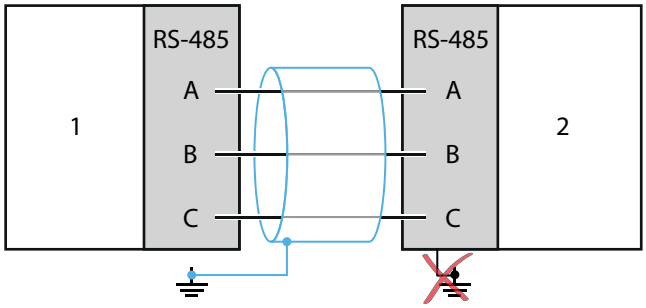
The cables recommended in the chapter Power supply line [▸ 5.3.1] have a foil screen and are designed based on S-UTP (screened unshielded twisted pair). The wire pairs are not individually shielded against each other (unshielded). Each pair comprises two color-coded wires that are twisted together (twisted pair).

NOTICE

It must be ensured that the screen is applied with the aid of the drain wire. The drain wire must be insulated to avoid short circuits on the circuit boards of the connected devices using a shrink-on tube or similar.

5.3.2.2 Connection RS-485

Lines A and B are arranged as a twisted wire pair.
Lines A and B must not be crossed.



1 Host control device 2 Compact Reader/Remote Reader

Do not ground the compact reader/remote reader.

5.3.2.3 Using several remote readers

If several Kaba Remote Reader 91 15 are to be connected to a host control device, either **bus wiring** or **star wiring** can be used.

See:

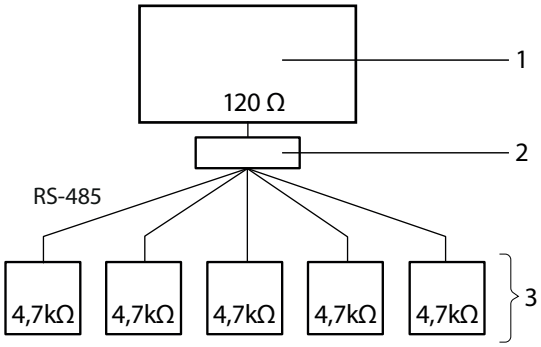
- Star wiring
- Bus wiring

5.3.2.4 Star wiring

Max. eight devices can be operated on a party line.

Power supply and data line in one cable: Maximum cable length per compact reader or stub: 20 m

Power supply and data line in separate cables: Maximum data line length per compact reader or stub: 100 m



1 Host control device
2 Distribution List
3 Compact Reader

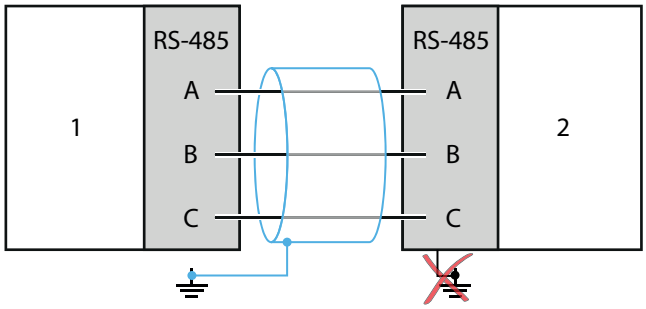
Installing terminating resistors

1. Set the terminating resistor to 120 Ω on the host control system (1).
   DIP Switch

2. For all devices (3) in the star wiring, set DIP switch 1 to **OFF** (open) and DIP switch 2 to **ON** (4.7 Ω).
   DIP Switch

Connecting shielding

1. On the host control device, connect the shielding of the RS-485 cable (blue) to the ground.
   Do not ground the compact reader.



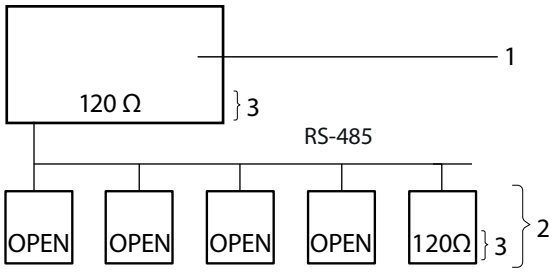
1	Host control device	2	Compact Reader

2. Connect all shieldings pertaining to the RS-485 cables used (blue) to each other.

5.3.2.5 Bus wiring

A maximum of eight devices can be operated on a party line.
Maximum total length of data lines (incl. stubs): 1200 m
A stub itself may be a maximum of 100 m in length.
The length of the party line can be increased using a repeater.

5.3.2.5.1 Bus wiring with 1 bus



1 Host control device
2 Compact Reader or Remote Reader
3 Terminating resistors

Installing terminating resistors

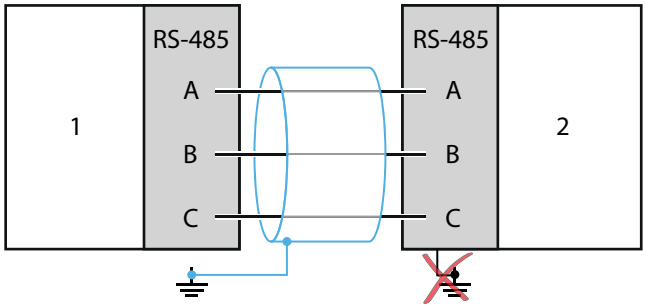
1. Set the terminating resistor to 120 Ω on the host control system (1).
2. On the last device in the bus wiring, set DIP switch 1 to **ON** (120 Ω), and DIP switch 2 to **OFF** (open).
3. On all other devices in the bus wiring, set DIP switch 1 and 2 to **OFF** (open).

Set peripheral address

1. Assign unique addresses to the devices connected to the bus.
   Set peripheral address [▸ 5.6.4]

Connecting shielding

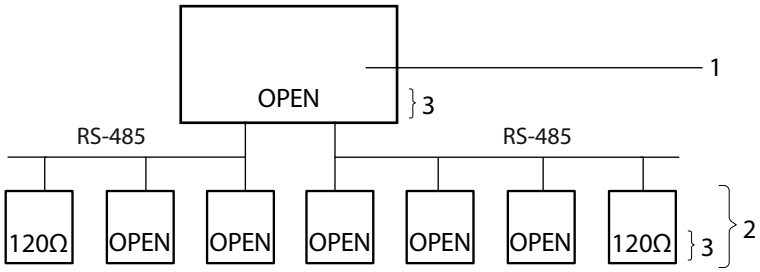
1. On the host control device connect the shielding of the RS-485 cable (blue) to the ground.
   Do not ground the compact reader/remote reader.



1 Host control device 2 Compact Reader, Remote Reader

2. Connect all shieldings of RS-485 cables (blue) used in the bus to each other.

5.3.2.5.2 Bus wiring with two buses



1 Host control device
2 Compact Reader or Remote Reader
3 Terminating resistors

Installing terminating resistors

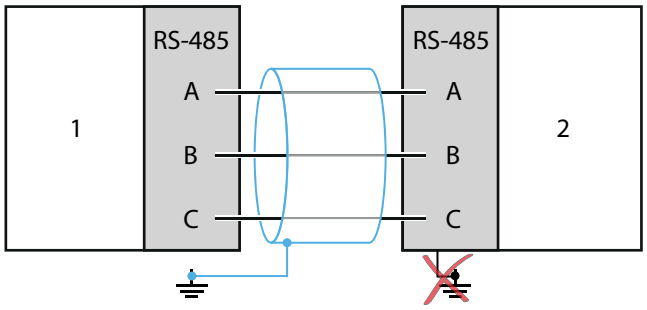
1. Set the terminating resistor to **OFF** (open) on the host control system.
2. On both terminal devices in the bus wiring, set DIP switch 1 to **ON** (120 Ω), and DIP switch 2 to **OFF** (open).
3. On all other devices in the bus wiring, set DIP switch 1 and 2 to **OFF** (open).

Set peripheral address

1. Assign unique addresses to the devices connected to the bus.
   Set peripheral address [▸ 5.6.4]

Connecting shielding

1. On the host control device connect the shielding of the RS-485 cable (blue) to the ground.
   Do not ground the compact reader/remote reader.



1 Host control device 2 Compact Reader, Remote Reader

2. Connect all shieldings of RS-485 cables (blue) used in the bus to each other.

5.3.3 Line to the door opener and door contacts

Line requirements: Cable diameters from 0.5 mm to 0.8 mm.

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

5.3.4 Coaxial Cable to the Registration Units

Cable Type RG174/U	Coaxial cable 50 Ohm, item No. 161.250 Maximum cable lengths: Cable type RG174: up to 30 m Cable type RG178/U: up to 30 m (RU 90 02: up to 10 m)
Recommended cable length	< 10 m
Max. cable length	30 m

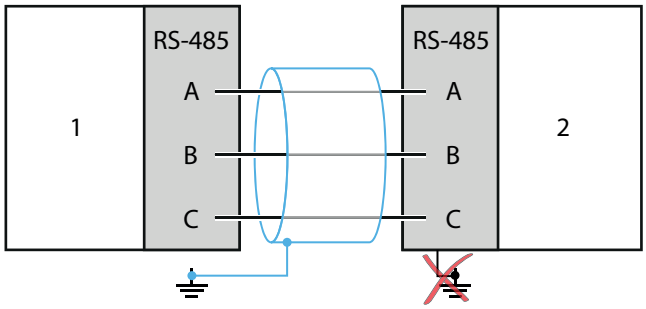
5.3.5 Grounding Concept

5.3.5.1 Power supply

The divice is in a plastic housing and is not grounded.
The power supply can be operated floating or grounded.

5.3.5.2 Communication lines

1. On the host control device connect the shielding of the RS-485 cable (blue) to the ground.
   Do not ground the Kaba Remote Reader 91 15.



1 Host control device 2 Kaba Remote Reader 91 15

1. Connect all shieldings pertaining to the RS-485 cables used (blue) to each other.

5.3.5.3 Coaxial Cable Terminal

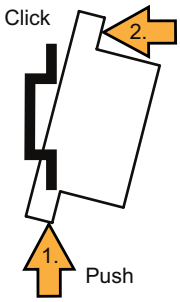
NOTICE

Inner conductor A+ and shield AS of the coaxial cable may be connected to the ground.

5.4 Mounting the device and extension modules

Mount the device on a 35 mm DIN rail (EN 50022).

1. Install the rail.
2. Screw grounding terminal to the rail.



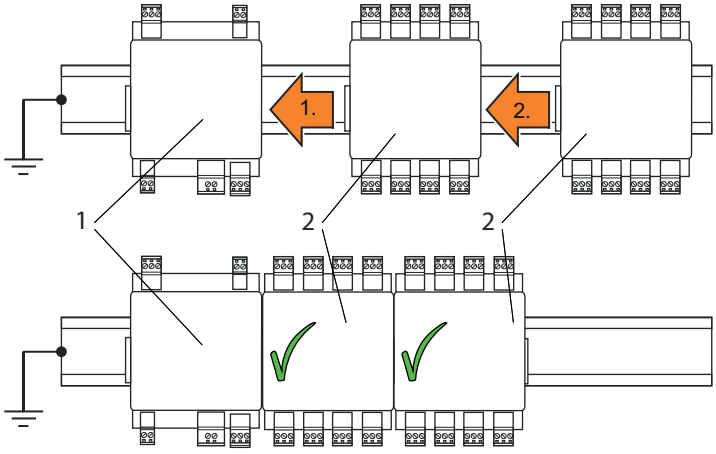
3. Hang the device on the bottom of the DIN rail – without tilting – and press it upwards and keep it pressed.
4. Press the device upwards against the rail at the same time until it can be hung on the rail.

Connecting extension modules

NOTICE

Attaching live extension modules may cause damage to the devices.

Always switch off the power supply before attaching the extension modules.



1 Kaba Remote Reader 91 15

2 Extension module 90 30

Connecting multiple 90 30 modules

1. Carefully insert the first extension module 90 30 into the device (1) (push the devices together on the rail).
2. Next insert the second extension module 90 30.

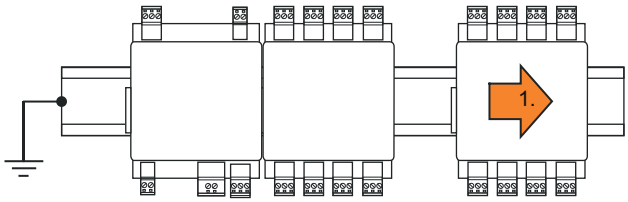
   ⇨ The extension module which is closer to the device (1) is designated as **Module 1**. The next module is designated as **Module 2**.

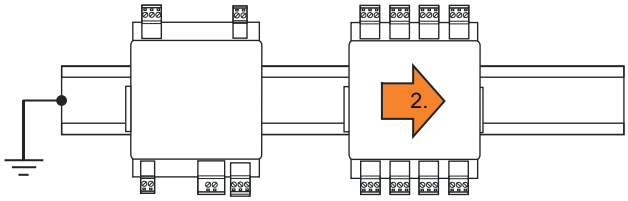
Removing extension modules

NOTICE

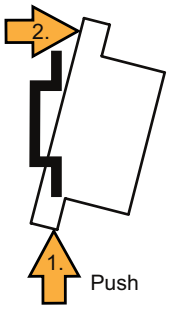
Removing live extension modules may cause damage to the devices.

Always switch off the power supply before removing the extension modules.





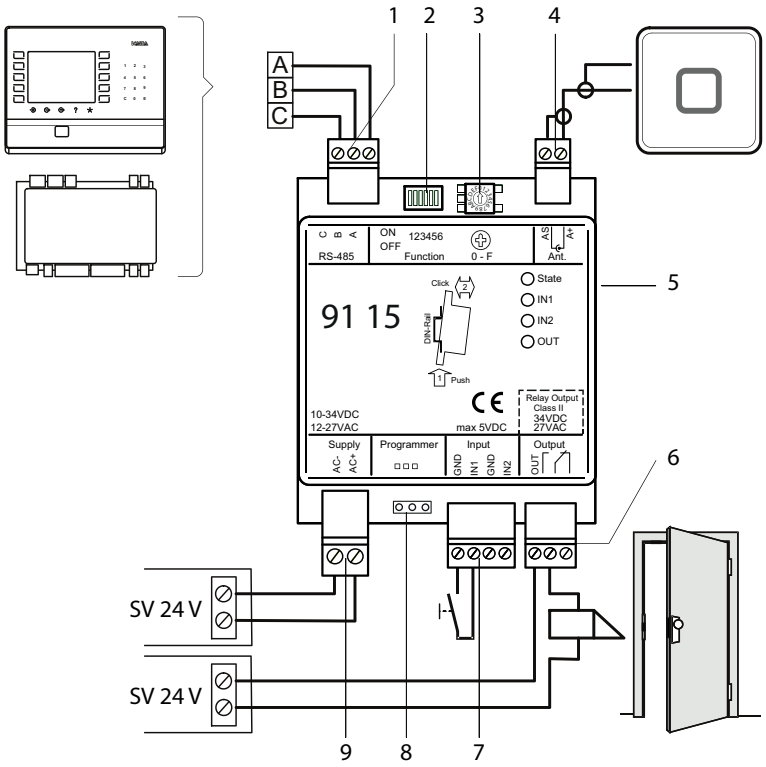
1. Push the extension module away from the adjacent module until the contact is fully disconnected.
2. Remove the disconnected extension module from the rail.



5.5 Connections

Only connect the terminals when the power is switched off.

5.5.1 Connections



Item	Connection/switch	Remark
1	RS-485 interface RS-485 line A RS-485 line B RS-485 line c (common)	Connection to the host system
2	Function	DIP switch for selecting the function
3	Addressing RS-485, 1–8	Rotary switch for selecting the address
4	Antenna	Registration unit
5	Interface for Extension Modules	e.g. 90 30/90 31
6	Relay output OUT	Contact load capacity 30 V AC/DC; max. 2 A
7	Digital input IN1: Door handle contact or door opener key REX	Connect to ground (GND) by means of a switch or relay contact.
	Digital input IN2: Frame contact FC	
8	Interface for Kaba programmer 1460	

Item	Connection/switch	Remark
9	Power supply	12–27 V AC (50/60 Hz) or 10–34 V DC
	Notice: The device may only be supplied with SELV (Safety Extra Low Voltage) and LPS (Limited Power Source), according to IEC/UL/CSA 60950-1.	

See also: Using several remote readers [▸ 5.3.2.3]
Set RS-485 termination resistances [▸ 5.6.3]

5.5.2 Inputs IN1–IN2

NOTICE

Connecting Isolated Inputs.

The function of the inputs and outputs depends on the control unit used and its parameter settings.

The logic (normally open [active low]/normally closed [active high]) of the inputs can be changed by the host system.

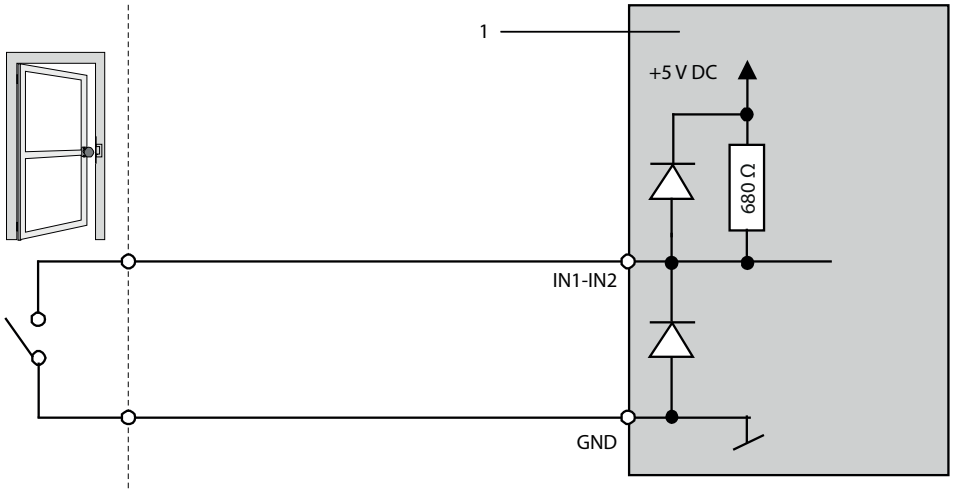
Allocation	Meaning
	GND (common ground)
IN1 (input 1)	Door handle contact or door opener key REX
IN2 (input 2)	Frame contact (FC)

If the Kaba Remote Reader 91 15 needs to behave in the same way in both online and offline operation, the inputs and relay outputs must be connected according to the operating mode and configured with the DIP switches.

DIP switches 3 and 4 define the function of inputs IN1 and IN2.
DIP Switch

IN1 and IN2 can, when necessary, be used as line-monitored inputs.
Inputs IN1–IN2 With Line Monitoring [▸ 5.5.2.2]

5.5.2.1 Inputs IN1–IN2 (Without Line Monitoring)



1 Kaba Remote Reader 91 15

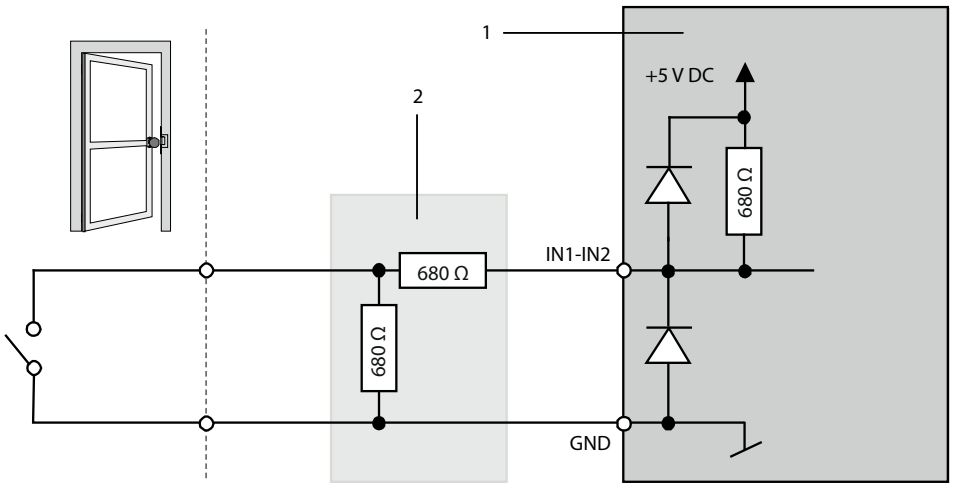
Internal wiring without line monitoring

Example: Connection of door frame contact not line monitored.
Any tampering with the lines between Kaba Remote Reader 91 15 and the door frame contact is not detected.

5.5.2.2 Inputs IN1–IN2 With Line Monitoring

Any tampering with the lines between the Kaba Remote Reader 91 15 and, for example, the door frame contact is detected.

1. **Activate/deactivate line monitoring:**
   On the host system, activate or deactivate line monitoring for each input.
2. **Inputs with line monitoring:**
   Attach resistors (R=680 Ω, ¼ W 2%), ensuring they are tamper-proof.



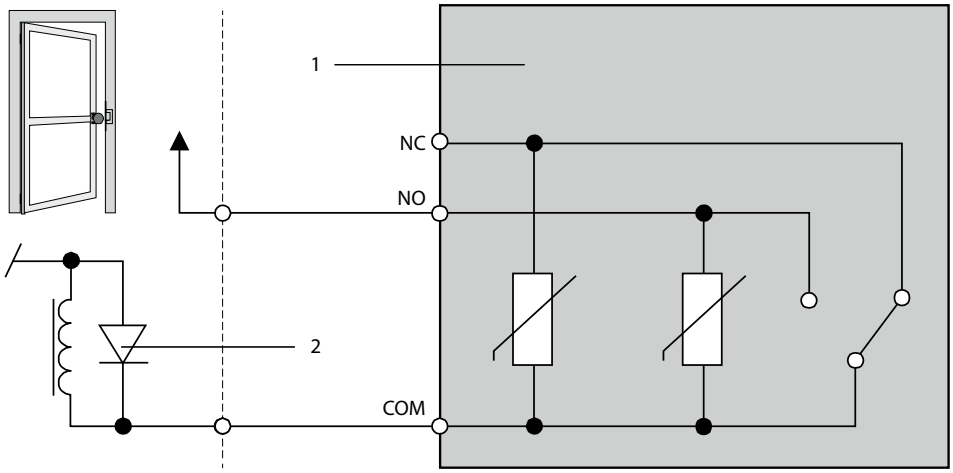
1 Kaba Remote Reader 91 15
2 Tamper-proof area

3. **Using inputs with and without line monitoring at the same time:**
   No resistors need to be connected to lines without line monitoring.

5.5.3 Output

The function of the inputs and outputs depends on the control unit used and its parameter settings.

Output (OUT), e.g. for an electric strike:



1 Kaba Remote Reader 91 15

2 Free-wheeling diode for door openers with DC voltage
or
varistor for door openers with AC voltage.

Item*	Meaning
6	NC (normally closed)
6	COM
6	NO (normally open)

*See

Contact load capacity: See Outputs

Also see about this

5.5.1 Connections [▸ 43]

5.5.3.1 Note on the use of door openers

The relay can be used to activate the door opener. For door openers that are supplied with DC voltage, a "free-wheeling" diode must be parallel-connected (in the reverse direction) to the door opener for noise attenuation. A varistor must be connected parallel to AC voltage door openers.

5.6 Configuration

5.6.1 Directions for configuration

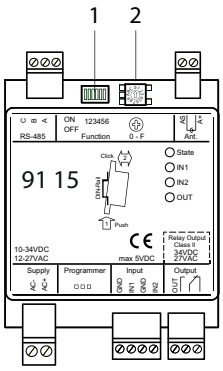
The switch settings determine the behavior of the device.

NOTICE

Switch settings may only be changed while the device is powered down.

Changed settings will only be adopted after an interruption to the power supply.

5.6.2 Switch



1 DIP switch (selection of functions)

2 Rotary switch (addressing)

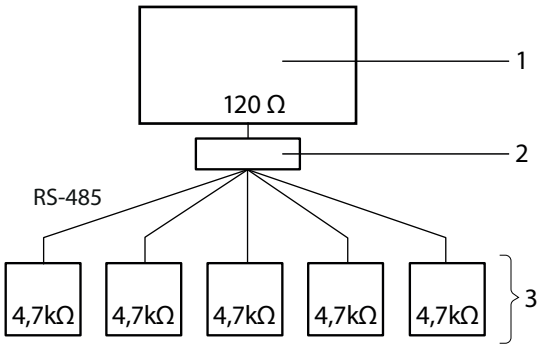
1. Set the device's switch in accordance with the following description.

5.6.3 Set RS-485 termination resistances

The connection architecture determines the terminating resistors.

1. Set terminating resistors in accordance with the following description.

Star wiring



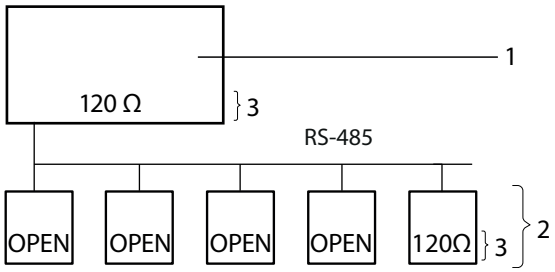
1 Host control device (Kaba access manager AM)
2 Distributor (e.g. screw terminal)
3 Terminating resistors Kaba Remote Reader 91 15

1. Set the terminating resistor to 4.7 kΩ on all Kaba Remote Reader 91 15 (3).

DIP switch number	Position	Effect
1	ON	Terminating resistance 4.7 kOhm (star wiring)
2	OFF	open

1. Set the terminating resistor to 120 Ω on the host control system (1).

Bus wiring with 1 bus



1 Host control device (Kaba access manager AM)
2 Kaba Remote Reader 91 15
3 Terminating resistors

1. Set the terminating resistor to 120 Ω on the last Kaba Remote Reader 91 15 of the bus wiring.

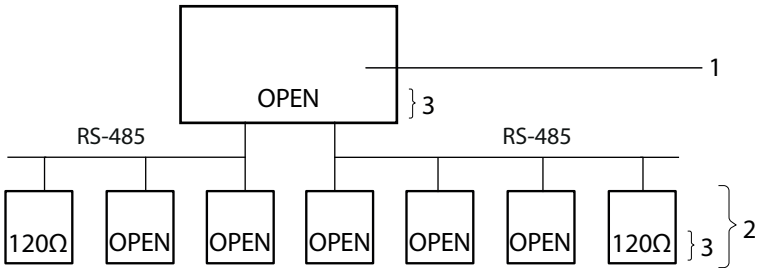
DIP switch number	Position	Effect
1	ON	Terminating resistance 120 Ohm
2	OFF	open

1. Set the terminating resistor to **open** on all other Kaba Remote Reader 91 15 of the bus wiring.

DIP switch number	Position	Effect
1	OFF	open
2	OFF	open

1. Set the terminating resistor to 120 Ω on the host control system.

Bus wiring with two buses



1 Host control device (Kaba access manager AM)
2 Kaba Remote Reader 91 15
3 Terminating resistors

1. Set the terminating resistor to 120 Ω on both terminal devices of the bus wiring.

DIP switch number	Position	Effect
1	ON	Terminating resistance 120 Ohm
2	OFF	open

1. Set the terminating resistor to **open** on all other Kaba Remote Reader 91 15 of the bus wiring.

DIP switch number	Position	Effect
1	OFF	open
2	OFF	open

1. Set the terminating resistor to **open** on the host control system.

5.6.4 Set peripheral address

Each device connected to an RS-485 bus must have a unique address.

1. Set a unique device address on the rotary switch.

Position	Peripheral address	Position	Peripheral address
0	Default, not used	5	5
1	1	6	6
2	2	7	7
3	3	8	8
4	4	9–F	Not used

1. Note down the address. It is required for configuration in the host system.

5.6.5 Settings for “Electric strike” operating mode

The door configuration determines the operating mode of the Kaba Remote Reader 91 15.
The operating mode is set with the DIP switch.

If the device is intended to support simplified door management in offline mode, inputs 1 and 2 must be connected in accordance with chapter , and defined according to the description in this chapter.

DIP switches 3 and 4 define the behavior of the connections IN1, IN2 and OUT.

1. Parameterize the access point in the system in accordance with “Connection of Electric Door Strikes”.
2. Set DIP switches 3 and 4.

DIP switch number	Position	Function	Connection
3	ON	Door frame contact (FC) active	IN2
	OFF	-	-
4	ON	REX; Door opener key	IN1
	OFF	Door handle contact	IN1

IN1 and IN2 can, when necessary, be used as line-monitored inputs.

See

5.6.6 Activate the monitoring of inputs

Line monitoring can only be activated and deactivated by the host system.

1. Activate line monitoring in the host system.

6 Start-up

6.1 "Standalone Access Control without Host System" Commissioning

(Construction site mode)

The Remote reader can already be used on a host system even before connection. This enables the use of the remote reader, e.g., during the construction phase.

By connecting the remote reader to a host control device (host system), the functions of the remote reader described in this chapter are replaced by parameterization of the system.

6.1.1 Using LEGIC

If using "Standalone access control (without host system)", only the LEGIC stamp (segment search key) is checked. To authorize access, the user medium's stamp must match the stamp of the remote reader.

- If using "Standalone access control (without host system)" the remote reader can only be used with one stamp (segment search key).

Preparation

1. Use security card C1 (IAM) to define the stamp of master A (only LEGIC ISO 14443A) (see RM_LEGIC_advant_Media_Definition).

Putting into operation

1. Carry out factory reset on the remote reader, see Chapter
2. Present Master A (only LEGIC ISO 14443A) to the connected registration unit
   - ⇨ In the event of successful transfer of the stamp: 3x short beep
   - ⇨ The stamp (segment search key) was transferred onto the remote reader
   - ⇨ The remote reader is now ready for bookings

Functions

- Book
- Save the following events (max. 2000):
  - Door forced open
  - Doors opened using the button/door handle
  - Door open too long
- Not saved:
  - Access events
  - The time and date stamps are incorrect/invalid because the clock on the remote reader has not been set yet.

Book

1. Present a LEGIC user medium (LEGIC prime, ISO 14443A or ISO 15693) to the connected registration unit.
   - ⇨ If the stamp (segment search key) of the remote reader matches a stamp of the user medium: Access authorized

6.1.2 Using MIFARE

If using "Standalone access control (without host system)", only the site key/fabrication key is checked. During the check, the medium's fabrication key is not replaced. To authorize access, the user medium's site key must match one of the remote reader's site keys.

- A security card C, a master A, or a master B medium can contain up to eight site keys.
- On the medium, the site key's identification file must match the "default ARIOS configuration"; the application ID, file ID, and coding of the identification number must match. Media with changed application IDs or non-standard identification number coding will not be recognized.

Putting into operation

1. Carry out factory reset on the remote reader, see Chapter
2. Hold security card C, a master A or a master B medium in front of the connected registration unit.
   - ⇨ In the event of successful transfer of the stamp: 3x short beep
   - ⇨ A maximum of eight site keys are transferred onto the remote reader
   - ⇨ The remote reader is now ready for bookings

Functions

- Book
- Save the following events (max. 2000):
  - Door forced open
  - Doors opened using the button/door handle
  - Door open too long
- Not saved:
  - Access events
  - The time and date stamps are incorrect/invalid because the clock on the remote reader has not been set yet.

Book

1. Present a MIFARE user medium (MIFARE DESFire or MIFARE classic) to the connected registration unit.
   - ⇨ The user medium's site key must match one of the remote reader's site keys: Access authorized

6.2 Issue Write/Read Authorization (Launch)

(LEGIC only)

A write/read authorization is required in the following cases:

- If the Remote reader needs to write on a write-protected segment of a medium, e.g. in the case of CardLink applications, validate write-protected CardLink segments
- If the Remote reader needs to read a read-protected segment of a medium

In this chapter, the term "Write authorization" will be used for the terms "Write authorization" and "Read authorization".

Write authorization with a LEGIC prime SAM 63 card is only valid for LEGIC prime.

Write authorization with a LEGIC advant SAM 63 card is only valid for LEGIC prime and LEGIC advant 15693 and 14443A.

In this chapter, the designation "Security card C2" will be used for the card designations "SAM 63" and "Security card C2 (SC-C2)".

The signaling is carried via the registration unit on which the card is presented.

Requirements

- For the write authorization, a security card C2 with corresponding segment area is required.
- ISO standard 14443A must have been activated using security card C2.
- The ISO standard of the SAM 63 card must match the parameterized ISO standard.
- The Remote reader should be in regular operation and waiting for an RFID entry.

Procedure

1. Present the security card C2 to the connected registration unit without interruption (approx. 15 s).
   - ⇨ The Registration unit illuminates green during the process.
   - ⇨ Signaling after successful write authorization: 3x beeps
     If the Remote reader has previously been granted write authorization using the same security card C2, this will be signaled immediately by 3x beeps
   - ⇨ No signaling: Write authorization has **not** been granted.
     Possible reasons
     - The security card C2 card was removed from the RFID field too early
     - ISO 14443A is not activated in the system
     - If SAM+ media are being used: No credit is available
2. Remove the security card C2 from the field.

6.3 Cancel Write/Read Authorization

(Only for LEGIC Compact Reader)

The write/read authorization needs to be canceled in the following cases:

- If the Remote reader no longer needs to write on write-protected segments of a medium

- If the Remote reader no longer needs to read read-protected segments of a medium

In this chapter, the term "Write authorization" will be used for the terms "Write authorization" and "Read authorization".

In this chapter, the term "Writing right" will be used for the terms "Writing right" and "Reading right".

6.3.1 Cancel all writing rights granted by a write authorization

1. Reset remote reader to the basic status, see Chapter

6.3.2 Cancel a particular writing right granted by a write authorization:

Use the SAM 64 card to delete the relevant stamp.

The signaling is carried via the registration unit on which the card is presented.

Requirements

- In order to cancel the write authorization, a SAM 64 card with the relevant segment range is required.
- The Remote reader should be in regular operation and waiting for an RFID entry.

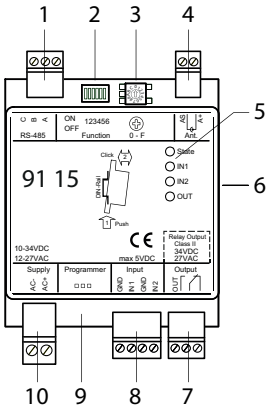
Procedure

1. Present the SAM 64 card to the connected registration unit without interruption (approx. 15 s).
   - ⇨ The Registration unit illuminates green during the process.
   - ⇨ 3x beep: Write-authorization canceled
     If the write authorization has already previously been canceled with the same SAM 64 card, this will be signaled immediately with 3x beeps.
   - ⇨ No signaling: Write authorization has **not** been canceled.
     Possible reasons
     - The SAM 64 card was removed from the RFID field too early
     - ISO 14443A is not activated in the system
     - If SAM+ media are being used: No credit is available
2. Remove the SAM 64 card from the field.

7 Maintenance

7.1 Programming interface

The Kaba Remote Reader 91 15 has a three-pin socket (9) for connecting a Kaba programmer. This programming interface is used, for example, for firmware updates.



7.2 Restart

Consequences of the restart

- Duration approx. 3 seconds
- The access point is blocked during the restart.
- The saved parameter settings and data remain in place.
- The device is restarted.

1. Switch the power supply off and on again.
   - ⇨ The LED **state** goes out.
   - ⇨ The access point is blocked.
2. After the restart, the LED **state** changes back to green.
   - ⇨ **Offline mode:** If the device is parameterized for offline mode, the access point is now ready for bookings.
   - ⇨ **Online mode:** After the connection has been set up with the host control device, the remote reader is ready for operation in online mode.

Restarting resets the internal clock. After restarting, the clock will read 01/01/2010 00:00. Logbook entries will be saved with an incorrect date stamp as a result until the next online operation.

7.3 Factory Reset/Reset Device to the Basic Status

Consequences of the factory reset

- The device is returned to its basic state (factory settings).
- The parameter settings are deleted.
- The stamps are deleted.
- The factory reset lasts approximately 3 seconds.
- The access point is blocked during the factory reset.

Procedure	Signaling Remote reader	Signaling Registration unit
1. Disconnect the device from the power supply.		
• The access point is blocked during the factory reset.		
2. Set DIP switch 6 to **ON**. (Switching the DIP switch when the power supply is connected has no effect).		
3. Connect the device to the power supply.		
	After the registration unit beeps, all LEDs flash orange	2 x short beep, then red/green flashing
• Device is reset to the factory settings (for further effects, see above, consequences of the factory reset).		
4. Disconnect the device from the power supply.		
5. Set DIP switch 6 to **OFF**.		
6. Connect device to the power supply.		
• The device is in operation again. • In the event of online connection: The host control device loads the current parameters on the remote reader. • The access point is ready for bookings.	State: permanent green or flashing green or flashes alternating green/orange	permanent green

7.4 Firmware Update/LEGIC OS Update

An update can be performed in the following ways:

- Using the access manager service tool via access manager (via Ethernet and the RS-485 interface)
- Using the Kaba EAC service tool and programmer 1460

NOTICE

Consequences of the firmware update:

- Device is reset to the factory settings(basic status)
- The parameterization is deleted
- The data is deleted
- The stamps are deleted

7.4.1 Firmware update/LEGIC OS update via access manager

The firmware/LEGIC OS is updated using the **access manager service tool** via access manager (via Ethernet and the RS-485 interface). The access manager reference manual describes the process.

7.4.2 Firmware Update / LEGIC OS Update with programmer 1460

The firmware update/LEGIC OS update lasts around 120 seconds.

Requirements

- The firmware has been transferred from the Kaba EAC service tool to the programmer 1460 (the LEGIC OS is integrated into the firmware).
- The user is familiar with the handling of the programmer and the Kaba EAC service tool.
- Kaba EAC service tool ≥ V 2.6.1 is installed.
- FTDI driver (using the operating system) for Kaba programmer 1460 is installed (FTDI CDM supports D2XX and VCP functionality) http://www.ftdichip.com/FTDrivers.htm
- Microsoft .Net Framework 4 Client Profile is installed http://www.microsoft.com/net/

Procedure	Signaling Remote reader	Signaling Registration unit
1. Disconnect the device from the power supply. (Switching DIP switch 6 when the power supply is connected has no effect.) • The access point is blocked during the firmware update.		
2. Turn DIP switch 6 to **ON**. • Service mode is activated.		
3. Connect the device to the power supply.		

		All LEDs flash orange	2 x short beep, then alternate red/green flashing
		If the programmer is connected before switching on the power supply, then there is no flashing.	If the programmer is connected before switching on the power supply, then there is no flashing.
4.	Connect the programmer to the device using the programming cable.		
		LED off	Flashing stops, 1x short beep, LED briefly flashes green twice

NOTICE

During the firmware update, the power supply and the connection to the programmer must not be interrupted.

5.	On the programmer, select the firmware to be transferred and then **download**.		
	After successful download:		1x short beep, LED briefly flashes green twice
6.	Disconnect the device from the power supply.	If the programmer is removed before the power supply is interrupted, then the LEDs flash according to the update mode.	If the programmer is removed before the power supply is interrupted, then the LEDs flash according to the update mode.
7.	Set DIP switch 6 to **OFF**.		
	• Service mode is deactivated.		
8.	Disconnect the programmer from the device.		
9.	Connect the device to the power supply.		
	• The device is in operation again. • In the event of online connection: The host control device loads the current parameters on the remote reader. • The access point is ready for bookings.	State: permanent green or flashing green or flashes alternating green/orange	permanent green

7.5 Updating configuration

With an online connection, the host control unit downloads the current parameters to the reader.

7.6 Crossgrade

A crossgrade can be used to amend the functional type of a device. For example, a device with the functional type access manager (AM) can be turned into a device with the functional type E300 V4 or subterminal.

The process for changing the functional type is described in the user manual for Kaba programmer 1460, document no k1evo809.

7.6.1 Device with Bxxx firmware (MRD)

Remote reader before crossgrade			**Remote reader after crossgrade**	
	Functional type			**Functional type**
MRD (multi RFID device)	• AM • E300 V4 • Subterm. • AMC • NTU300 V3	Crossgrade ⇨	MRD (multi RFID device)	• AM • E300 V4 • Subterm. • AMC • NTU300 V3

Illustrative example

Only **B**xxx firmware (MRD) can be transferred to a device with **B**xxx firmware (MRD).
It is possible to change functional type.
It is possible to change between LEGIC and MIFARE.

7.6.2 Device with Axxx firmware (LEGIC)

Remote reader before crossgrade			**Reader type after crossgrade**	
	Functional type			**Functional type**
LEGIC	• AM • E300 V4 • Subterm. • AMC • NTU300 V3	Crossgrade ⇨	LEGIC	• AM • E300 V4 • Subterm. • AMC • NTU300 V3

Illustrative example

Only **A**xxx firmware (LEGIC) can be transferred to a device with **A**xxx firmware (LEGIC).
A change of functional type is possible.
A change from LEGIC to MIFARE is **not** possible.

7.6.3 Device with Mxxx firmware (MIFARE)

Remote reader before crossgrade			**Remote reader after crossgrade**	
	Functional type			**Functional type**
MIFARE	• AM • E300 V4 • Subterm.	Crossgrade ⇨	MIFARE	• AM • E300 V4 • Subterm.

Illustrative example

Only **M**xxx firmware (MIFARE) can be transferred to a device with **M**xxx firmware (MIFARE).
A change of functional type is possible.
A change from MIFARE to LEGIC is **not** possible.

8 Troubleshooting

8.1 LED Displays on the Remote Reader

LED designation	LED signaling	Meaning	Measures
State	green	Offline, in operation	
	green flashes	Online, in operation	
INx	green	Input aktive, ON	
	off	Input inaktive, OFF	
OUT	green	Relay aktive	
State	red permanent	• Incorrect firmware • Remote reader defective	• Carry out firmware update • Replace remote reader
	flashes green and orange	After an interruption in communication, until the Kaba Remote Reader 91 15 is queried for the first time by the host system	
	orange permanent	Service mode	
IN1–IN2 (only with monitored lines) (Assignments: IN2 to IN1 IN1 to IN2)	orange permanent	Short circuit	Check lines, line monitoring and resistances
	red permanent	Interruption	

8.2 During Installation

Error	Possible cause	Measures
Host system does not recognize the remote reader	Communication between remote reader and host system defective	Check communication using the LED state and adjust
	The address set on the remote reader does not match the address set in the system	Check address settings on the remote reader and in the host system
	Incorrect termination resistances	Adjust RS-485 termination resistances
	Interruption	Check/repair cable and connections

Error	Possible cause	Measures
Remote reader does not read correctly	Interruption	Check/repair connection of registration units
	Incorrect customer medium used	Check whether the correct customer medium was used when putting it into operation
	Medium does not match the definition in the system	Check whether the medium found and its definitions are parameterized correctly in the system
	Several devices which are connected to the RS485 bus have the same address	Give a unique address to each divice which is connected to the RS485 bus
	RF standard not parameterized in the host system	Adjust the configuration in the host system

8.3 During operation

Error	Possible cause	Measures
Host system does not recognize or only temporarily recognizes the Remote reader	Facility changed by user	Adjust facility
	New sources of interference (e.g. new or replaced hubs, cash dispensers or other security systems)	Reduce influence of the sources of interference (increase distance, shielding)
	Cabling changed	Adjust cabling
	Configuration of the access point in the host system changed	Adjust configuration of the access point in the host system
	Several devices connected to the RS-485 bus have the same address	Assign a unique address to each device connected to the RS-485 bus
Remote reader does not read correctly	Facility changed by user	Adjust facility
	New sources of interference (e.g. new or replaced hubs, cash dispensers or other security systems)	Reduce influence of the sources of interference (increase distance, shielding)
	Cabling changed	Adjust cabling
	Incorrect handling of the medium	Inform user of correct use of the medium and the registration unit
		RF standard not set correctly
	Structure of the medium or its structure in the system not correct	Adjust structure of the medium or its structure in the system

Error	Possible cause	Measures
Time sequence of the access point control is incorrect	Configuration of the access point in the host system changed	Adjust DIP switch settings
	Memory of the remote reader deleted via factory reset and the data of the host system has not yet been written to the remote reader	Adjust times in the host system and transfer to the remote reader
		Check whether the data has been loaded from the control device onto the remote reader after a factory reset
		Check whether the desired times have been defined in the host system
	Cabling changed	Adjust cabling
Remote reader does not write on the media	Remote reader has no write authorization	Grant write authorization
	CardLink settings in the host control device are incorrect	Adjust the configuration of the host control device

9 Packaging/Return

Incorrectly packaged assemblies and devices may cause expenses due to damage during transport.

Please observe the following information when sending Kaba products.

Kaba shall not be liable for damage to products which can be attributed to insufficient packaging.

10 Disposal

This chapter provides important information on disposal.

10.1 Decommissioning

The following steps should be executed for the decommissioning of the device in an access control system:

1. For online operation: Check configuration of the host system
2. Disconnect the device from the power supply
3. Disconnect RS-485 connection from the host system

10.2 Dismantling

1. Dismantle the device
   Dismounting

NOTICE

After dismantling:

Check the terminating resistors of all devices connected to the host control device.
Check the configuration of the host system.

10.3 Disposal

This product meets the requirements of the WEEE Directive and, in accordance with DIN standard EN 50419, is labeled with the WEEE crossed-out garbage can symbol.

The symbol indicates the separate disposal of electric and electronic equipment in EU countries.

Do not dispose of the device with household waste under any circumstances.

Used devices contain valuable recyclable materials that should be recycled. Used devices should therefore be disposed of via the collection system used in your country.

Disposal in Germany:
After use, Kaba GmbH undertakes to carry out the proper disposal of the supplied goods in line with legal requirements (such as the ElektroG law in Germany). All costs incurred for the transport of goods to the manufacturer's plant will be borne by the owner of the used electronic equipment.

Disposal in Switzerland:
Send the device to an electronic equipment collection facility as per the VREG regulation.

In the EU, electrical devices should be disposed of in accordance with national waste disposal and environmental directives.

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

Dispose of packaging in an environmentally-friendly manner.

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

Index

C

CE conformity 20
Conformity 20
Control 26

D

Designated use 11
Device address 50
Disposal 67
Door contact 32
Door frame contact 32
Door opener 32, 46

E

Electromagnetic fields 31
EMC directive 20
ESD protective measures 12
Extension modules, max. number 17

F

Factory reset 57
Firmware update 58

G

Grouped safety messages 11

I

Identification plate 22
Installation cables 32

L

LED Display 63
LEGIC OS update 58
Low voltage directive 20

O

Offline operation 28
Online operation 28

P

Packaging 66
Power supply line 33
Programming interface 56

R

R&TTE directive 20
Return 66
RFID reader 23
RoHS 20
Rotary switch 50
RS-485 bus termination 48

S

Safety 11
Safety messages 11
Supplementary Documentation 7

T

Troubleshooting 63