

**Annex acc. to FCC Title 47 CFR Part 15  
relating to  
dormakaba EAD GmbH  
dormakaba access manager 9200-K7**

# **Annex no. 5 User Manual Functional Description**

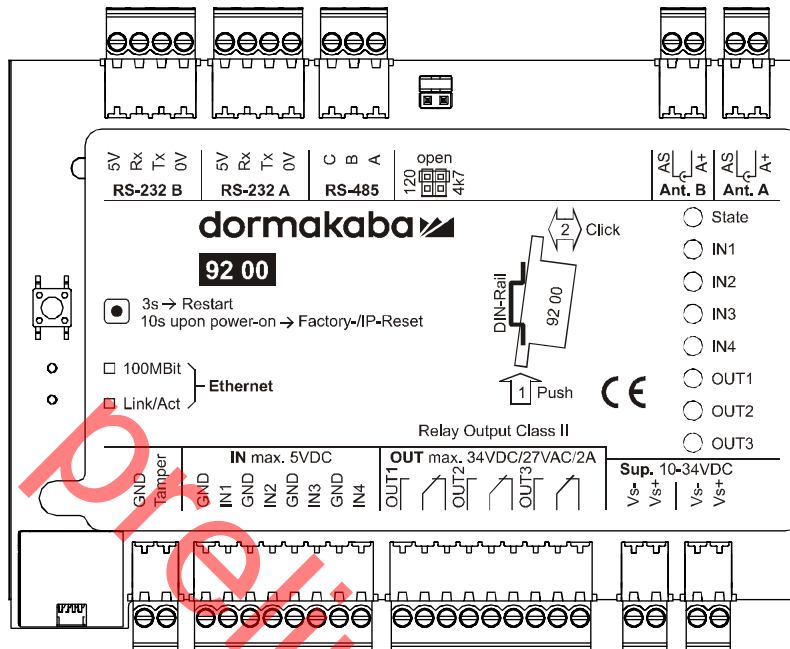
**Title 47 - Telecommunication  
Part 15 - Radio Frequency Devices  
Subpart C – Intentional Radiators  
ANSI C63.4-2014  
ANSI C63.10-2013**



Deutsche  
Akkreditierungsstelle  
D-PL-12053-01-03

EUT: dormakaba access manager 9200-K7      FCC ID: NVI-DKAM9200K7      FCC Title 47 CFR Part 15      Date of issue: 2020-11-13

**User Manual / Functional Description of the test equipment (EUT)**



# dormakaba

## access manager 92 00

### MATRIX – TP4-Client

## Technical Manual

04047408 - 10/2020

9200-K7 TP4-Client

EN

dormakaba

preliminary

Copyright © dormakaba 2020  
All rights reserved.

No part of this document may be reproduced or used in any form or by any means without prior written permission of dormakaba Schweiz AG.

All names and logos of third-party products and services are the property of their respective owners.

Subject to technical changes.

# Table of Content

<b>1</b>	<b>About this document</b>	<b>5</b>
1.1	Validity	5
1.2	Target group	5
1.3	Contents and purpose	5
1.4	Additional documentation	6
1.5	Availability of additional documentation	7
1.6	Orientation in the document	7
1.7	Instructions	7
1.8	Abbreviations/term definitions	8
1.9	Warnings	9
	1.9.1 Hazard categories	9
	1.9.2 Symbols	9
1.10	Notes	9
<b>2</b>	<b>Basic safety instructions</b>	<b>10</b>
2.1	Assembly and installation	10
2.2	Service and maintenance	10
2.3	Accessories and spare parts	10
2.4	Electrical hazards	11
2.5	ESD prevention measures	11
2.6	Environmental protection	11
2.7	Data protection and IT security	12
<b>3</b>	<b>Product description</b>	<b>13</b>
3.1	Overview	13
3.2	Specification	14
3.3	Mobile Access system overview	16
3.4	Technical data	17
	3.4.1 Power supply	17
	3.4.2 Data retention in case of power failure	17
	3.4.3 Interfaces	17
	3.4.4 Frequency bands and transmission power	18
	3.4.5 Inputs	18
	3.4.6 Outputs	18
	3.4.7 Terminals	18
	3.4.8 Environmental conditions	18
	3.4.9 Mechanics	18
	3.4.10 Dimensions	19
3.5	Conformity	20
3.6	Identification	21
3.7	Open source information	22
3.8	Included in supplied package	23
3.9	Accessories	23
	3.9.1 Top hat rail power supply units	23
	3.9.2 Extension module 90 30	23
	3.9.3 Extension module 90 31	23
	3.9.4 Detection units	24
<b>4</b>	<b>Construction and function</b>	<b>25</b>
4.1	Device layout	25
4.2	Signal	26
	4.2.1 Device status	26
	4.2.2 Ethernet LEDs	26
	4.2.3 IN/OUT LEDs	26
4.3	Reading behaviour	27

4.3.1	Behaviour with two registration units	27
4.3.2	Behaviour of readers installed next to each other	27
4.3.3	Behaviour when several media are present in the field (anti-collision)	27
4.4	System requirements	27
4.4.1	Mobile Access system requirement	27
<b>5</b>	<b>Installation</b>	<b>28</b>
5.1	Installation requirements	28
5.1.1	General	28
5.1.2	Installation location	28
5.1.3	Connections	28
5.2	Installation lines	29
5.2.1	General requirements	29
5.2.2	Ethernet	29
5.2.3	Lines to RS-485 devices	29
5.2.4	Line to the door opener, the door opener key, and the door contacts	30
5.2.5	Coaxial cables to registration units	30
5.3	Mounting device and extension modules	31
5.4	Connections	33
5.4.1	Overview	33
5.4.2	Power supply	34
5.4.3	RS-485 port	35
5.4.4	Registration units	37
5.4.5	Inputs	38
5.4.6	Outputs	39
<b>6</b>	<b>Commissioning</b>	<b>40</b>
6.1	Network parameters	40
6.1.1	MAC address of the device	42
6.1.2	Change network parameters with 'MATRIX Device Scanner'	43
6.2	Configuration	45
6.3	Initialise the device for Mobile Access	46
6.4	Additional steps for Legic media technology	48
6.4.1	Grant read/write authorisation	48
6.4.2	Withdrawing read/write authorisation	49
<b>7</b>	<b>Maintenance</b>	<b>50</b>
7.1	Restart reader	50
7.2	Reset the device to factory settings	51
<b>8</b>	<b>Decommissioning</b>	<b>52</b>
8.1	Dismantling	52
<b>9</b>	<b>Packaging/return</b>	<b>53</b>
9.1	Complete devices	53
9.2	Electronic component assemblies	53
9.3	Labelling	54
<b>10</b>	<b>Disposal</b>	<b>55</b>
	<b>Index</b>	<b>56</b>

# 1 About this document

## 1.1 Validity

This document describes the product:

Product designation:	dormakaba access manager 92 00
Product code:	9200-K7
Article number:	04079201
HVIN:	04046944-2
Firmware:	TP4 ≥ V4.03

This document describes all product variants and all optional accessories and functions. Options are subject to a charge and are thus only available if they have been purchased. Additional accessories and functions may not be available on the date of publishing and may only be available for purchase at a later point in time.

## 1.2 Target group

This manual is intended for skilled persons only.

The descriptions are intended for skilled persons trained by the manufacturer. This manual is not a replacement for product training.

For reasons of equipment safety, the installation, maintenance and service measures described in this documentation should only be carried out by skilled persons in accordance with EN 62368-1 (Audio/Video, Information and Communication Technology Equipment – Part 1: Safety Requirements).

Skilled person is the designation for people who have the appropriate technical training and experience in setting up the equipment. Skilled persons are expected to use their training and experience to identify any risks to themselves and others that may arise while carrying out these activities, and to minimise these risks as far as possible. It is the skilled person's responsibility to ensure that the conditions stated by the manufacturer and the applicable regulations and standards are complied with when carrying out these actions.

This documentation is also used to provide information for persons with the following tasks:

- Project planning and project implementation
- Commissioning the product within the network
- Connecting the product to user software by programming customer applications
- Customer-specific adjustments with product parameterisation

## 1.3 Contents and purpose

Contents are limited to the assembly, installation, commissioning and basic operation of the product.

## 1.4 Additional documentation

### MATRIX system environment

<b>Planning</b>	Planning guideline <ul style="list-style-type: none"> <li>• Mobile Access</li> <li>• Wireless</li> </ul>
<b>System software</b>	User manual/online help <ul style="list-style-type: none"> <li>• MATRIX Professional</li> <li>• MATRIX One</li> </ul>
<b>Access manager</b> Function type: MATRIX – TP4 client	Technical manual <ul style="list-style-type: none"> <li>• Access manager 92 00 [9200-K5]</li> <li>• Access manager 92 00 [9200-K7]</li> <li>• Access manager 92 30 [9230-K5]</li> <li>• Access manager 92 30 [9230-K7]</li> <li>• Access manager 92 90 Rack [9290-K5]</li> <li>• Access manager 92 90 Rack [9290-K7]</li> <li>• Access manager 92 90 Wall [9290-K5]</li> <li>• Access manager 92 90 Wall [9290-K7]</li> </ul>
<b>Compact reader</b> Function type: Access manager	Technical manual, MATRIX – TP4-Client <ul style="list-style-type: none"> <li>• Compact reader 91 04</li> <li>• Compact reader 91 10</li> <li>• Compact reader 91 12</li> </ul>
<b>Remote reader</b> Function type: Access manager	Technical manual, MATRIX – TP4-Client <ul style="list-style-type: none"> <li>• Remote reader 91 15</li> <li>• Remote reader 91 25</li> </ul>
<b>S6-R reader</b>	Technical manual
<b>Interface 90 10</b> Function type: Access manager	Technical manual <ul style="list-style-type: none"> <li>• Interface 90 10</li> </ul>
<b>Reader Interface</b>	Technical manual
<b>Programmer 1460</b>	Technical manual
<b>Wireless Gateway 90 40</b>	Technical manual
<b>Terminals</b>	Technical manual <ul style="list-style-type: none"> <li>• 96 00</li> <li>• 97 00</li> </ul>
<b>Electronic fittings</b>	Technical manual <ul style="list-style-type: none"> <li>• c-lever (compact/pro/air)</li> <li>• XS-Fitting Pro</li> </ul>
<b>Electronic cylinders</b>	Technical manual <ul style="list-style-type: none"> <li>• Digital cylinder</li> <li>• XS-Cylinder Pro</li> </ul>

[XXXX-K#] = Product code

There are several generations of the devices under the same product name.



## 1.5 Availability of additional documentation

Additional documentation is available on the dormakaba extranet.

You will need a user account to access the extranet. A user account can be created directly. Detailed information about this is available on the homepage.

**dormakaba extranet**

<http://www.dormakaba.com/extranet-emea-en>



## 1.6 Orientation in the document

This document contains the following features to help find specific topics:

- The table of contents at the beginning of the document offers an overview of all topics.
- The header contains the associated main section.
- Cross references indicate the number of the section containing additional information. Example [ ▶ 5.7].
- An index in alphabetical order is given at the end of the document.

## 1.7 Instructions

Structure and symbols of the instructions are illustrated in the following example:

- ✓ Prerequisite
- 1. Step 1
  - ⇒ Interim result
- 2. Step 2
  - ⇒ Result

Preliminary

## 1.8 Abbreviations/term definitions

Abbreviation	document	Explanation
AoC	Access on Card	With Access on Card, the authorisations are saved to RFID media.
APIPA	automatic private IP addressing	Devices/computers automatically get an IP address if there is no DHCP server present.
-	Bluetooth®	An international transmission standard based on radio technology for contactless exchange of data.
DoC	Data on Card	With Data on Card, the data is written from devices to RFID media. Example: Capacity of batteries
DP1	Device Protocol 1	Protocol for data transfer via RS-485 bus.
KCP	Kaba Communication Protocol	Protocol for data transfer via RS-485 bus.
NFC	Near Field Communication	An international transmission standard based on RFID technology for contactless exchange of data.
RFID	Radio-Frequency Identification	Technology for transmitter-receiver systems for the automatic and contactless identification of objects with radio waves.
TP4	Terminal Protocol 4	Protocol for data transfer via RS-485 bus or Ethernet.
VCP	Versatile Configuration Package	Configuration package for Mobile Access

## 1.9 Warnings

Warnings containing information/instructions and prohibitions designed to prevent personal injury or damage are specially marked.

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

### 1.9.1 Hazard categories

Warnings are divided into the following categories:



#### **DANGER**

##### **High risk**

Indicates an imminent danger which could cause severe physical injury or death.



#### **WARNING**

##### **Medium risk**

Indicates a possibly dangerous situation which may lead to severe physical injury or death.



#### **CAUTION**

##### **Low risk**

Indicates a possibly dangerous situation which may lead to minor physical injury.



#### **NOTICE**

##### **Important information on the correct use of the product.**

Failure to comply with these instructions could lead to malfunctions. It is possible to damage the product.

### 1.9.2 Symbols

Symbols with the following meaning are used for warnings, depending on the source of danger.



General hazard



Hazard due to electrical current



Explosion hazard



Risk for electronic components due to electrostatic discharge

### 1.10 Notes

Notes are indicated by an info symbol.



Tips and useful information.

These help you make the best use of the product and its functions.

## 2 Basic safety instructions

This product has been built to state-of-the-art standards and in line with established safety regulations. However, hazards for persons and property may arise when handling the product.



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

### 2.1 Assembly and installation

Check the device for visible damage caused by transport or incorrect storage. Do not start up any damaged device!

Assembly and installation of the product may only be done by skilled personnel (see chapter 1 Target group).

Mains voltage installations may only be carried out by a certified specialised company or authorised electricians.

When installing/inserting the product in end-use equipment all requirements of the mentioned test standards must be fulfilled.

The product should only be installed in locations which fulfil the environmental and technical conditions specified by the manufacturer.

The manufacturer is not liable for damage arising due to improper handling or incorrect installation.

### 2.2 Service and maintenance

Conversions and modifications to the product may only be done skilled personnel (see chapter 1 Target group). Any conversions and modifications performed by other persons will exempt us from any liability.

The elimination of faults and maintenance work may only be performed by skilled personnel (see chapter 1 Target group).

### 2.3 Accessories and spare parts

Accessories and spare parts must meet the manufacturer's technical requirements. This is guaranteed if original dormakaba accessories and spare parts are used.

## 2.4 Electrical hazards



### **⚠ WARNING**

#### **Live connections in the area of the DIN rail power supply units**

Carelessness can result in an electric shock.

Before you carry out maintenance work on the open device, take the following measures:

- The installation area with power supply units for the device must only be accessible to skilled persons (see chapter 1 "Target group [▶ 1.2]").
- De-energize before starting maintenance work.
- Secure against being switched on again.
- Check for absence of voltage.

## 2.5 ESD prevention measures



### **NOTICE**

#### **Risk for electronic components due to electrostatic discharge.**

Incorrect handling of electronic PCBs or components can result in damage which will cause a complete breakdown or sporadic errors.

- General ESD prevention measures must be observed when installing or repairing the product.
- Wear an anti-static wrist strap when handling electronic components. Connect the end of the strap to a discharge box or a non-painted, earthed metal component. This way, static discharges are channelled away from your body safely and effectively.
- Handle a PCB along its edges only. Do not touch the PCB or connectors.
- Place dismantled components on an anti-static surface or in an anti-static shielded container.
- Avoid contact between PCBs and clothing. The wrist strap protects PCBs against an electrostatic discharge voltage from the body only. However, damage can also be caused by an electrostatic discharge voltage from clothing.
- Transport and ship dismantled modules in conductive anti-static bags only.

## 2.6 Environmental protection

It is prohibited to dispose of the device in your domestic waste.

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

Dispose of consumed batteries in accordance with state and local regulations.

Carefully store the batteries to be disposed of to avoid short circuits, crushing or destruction of the battery casing.

## 2.7 Data protection and IT security

The system software and the device must be configured for safe operation.

Unauthorised access to the device and the system is possible without further security settings.

### Security risks

- Data protection violation through unauthorised access to person-related data
- Unauthorised access
- Tampering/system failure

### Recommended measures

- Device:
  - Keep the firmware current.
  - Before decommissioning: Reset the device to factory settings.
- System software:
  - Activate encrypted communication.
  - Switch off network ports that are not required.
  - Follow the dormakaba MATRIX security hardening guide.
  - Copy the latest patches.



The recommended actions refer only to the linking of the dormakaba access managers to the MATRIX system software without making any claims as to completeness and currency.

The facility operator of the system must ensure the protection of person-related data and IT security in their entire organisation by taking suitable measures.

---

# 3 Product description

## 3.1 Overview

The device is used as an access control terminal in an access control system.

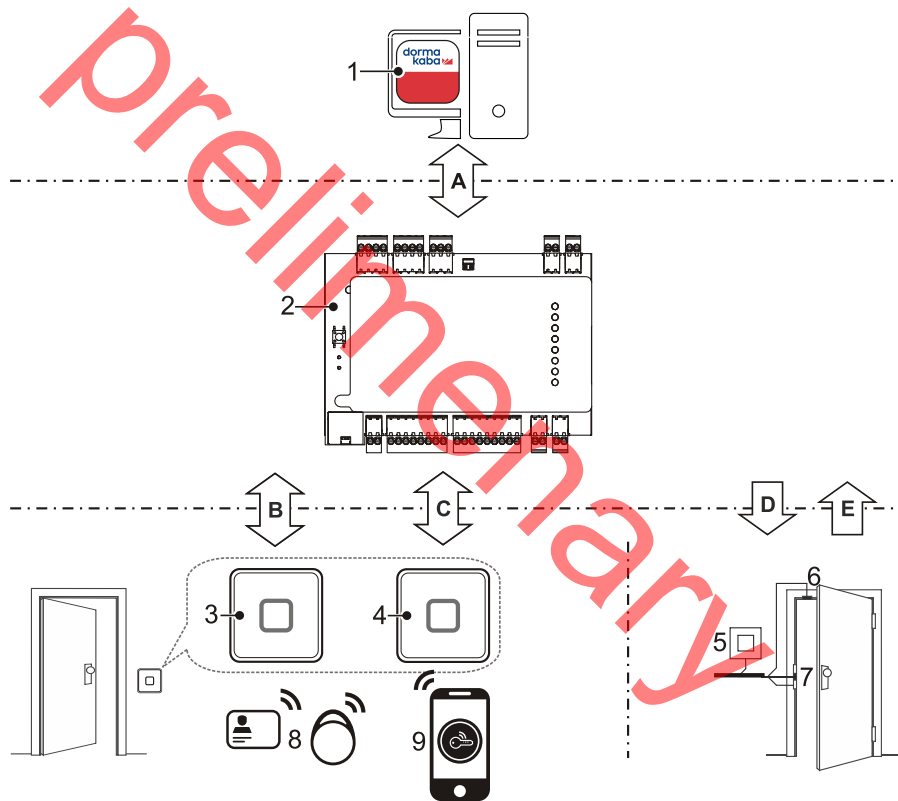
The access control system is managed with the system software. In the system software, the access permissions are assigned and the connected devices are configured. The access permissions are saved in the device.

More devices are connected to the device. The connected registration units/readers read the data from media. The device checks the permission of the media.

The device supports Mobile Access. With Mobile Access, smartphones with the dormakaba mobile access app become media.

If a medium is authorised, the device releases the access.

The doors status is identified and evaluated via the digital inputs of the device.



1	System software	6	Door frame contact
2	Access manager 92 00 (TP4 client)	7	Electric strike
3	Registration unit	Media	
4	Reader	8	ID card/key fob
5	Electric strike button	9	Smartphone

- A Access rights, bookings, notifications, configuration
- B Data from media, signalling
- C Data from media, signalling, configuration
- D Actuation of electric strike and other actuators
- E Signals from contacts

## 3.2 Specification

### System environment

- System software: MATRIX Professional/MATRIX ONE
- Access manager: TP4 client

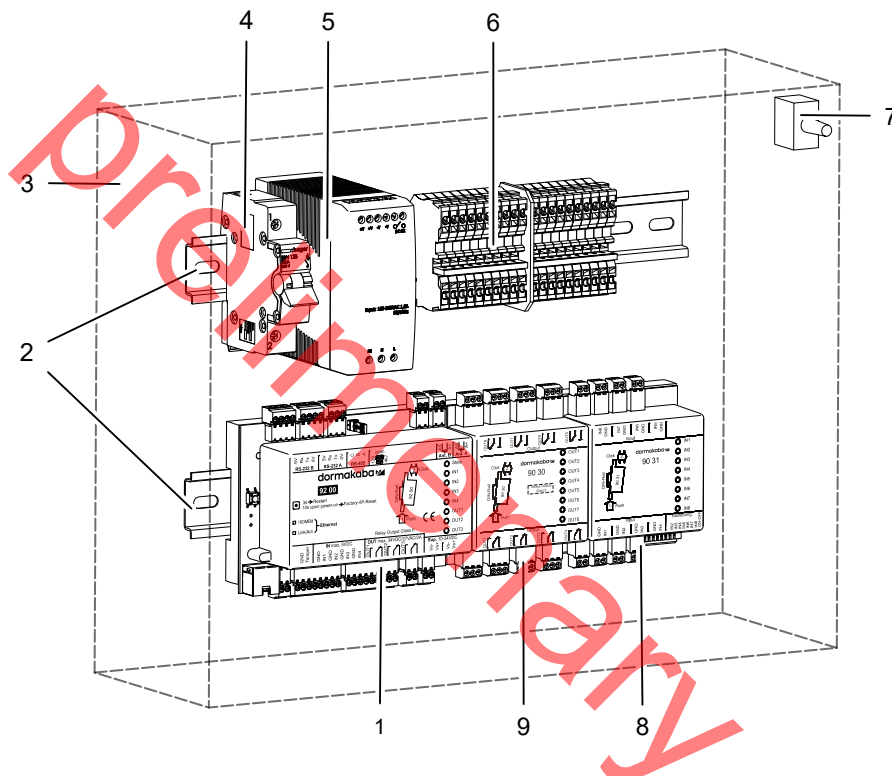
### Assembly

The device is fitted on a top hat rail inside a switch cabinet.

### Special feature

The device can be combined with other devices.

Example:



		dormakaba Product range	Outsourcing
1	Access manager 92 00	●	-
2	Top hat rail	-	●
3	Switch cabinet	-	●
4	Mains switch	-	●
5	Power supply unit	●	●
6	Terminal strips (power distribution)	-	●
7	Tamper switch	-	●
8	Extension module 90 31	●	-
9	Extension module 90 30	●	-
-	Other parts as required	-	●

● yes

- no



**Connections for readers/devices**

- 2x registration units 90 xx via the coaxial ports
  - Supported RFID technologies: Legic/MIFARE/FeliCa  
The RFID technology is set in the system software.
  - Supported functions: AoC, DoC, Mobile Access
- 1 RS-485 interface
 

The protocol is determined in the system software. Depending on the protocol, the following devices can be connected.

  - KCP: up to 15 devices  
compact reader 91 xx, remote reader 91 xx, interface 90 10  
Only readers with functional type 'Access Manager' are supported.
  - DP1: up to 16 devices  
S6-R reader
  - phgCrypt: Readers from third-party manufacturers
- 2 RS-232 interfaces
  - Reader with ASCII character transfer (9600 Baud, 8N1)  
e.g. barcode scanner

**Inputs/outputs**

- 4x digital inputs
  - For connecting insulated switches
  - Power supply integrated
- 3x output
  - Potential free switching contact

Optionally, the number of inputs and outputs can be increased with extension modules.

- The extension module 90 30 has eight additional outputs.
- The extension module 90 31 has eight additional inputs.

The extension modules are plugged into the device and are simultaneously connected electrically.

The table indicates the quantity of extension modules and their combination options.

Extension	Extension modules		Inputs/outputs	
	Maximum number		Total available	
	90 30	90 31	Outputs	Inputs
Only extension module 90 30	9	0	75	4
Only extension module 90 31	0	5	3	44
Extension module 90 30 + 90 31	2	2	19	20

**Security against attacks**

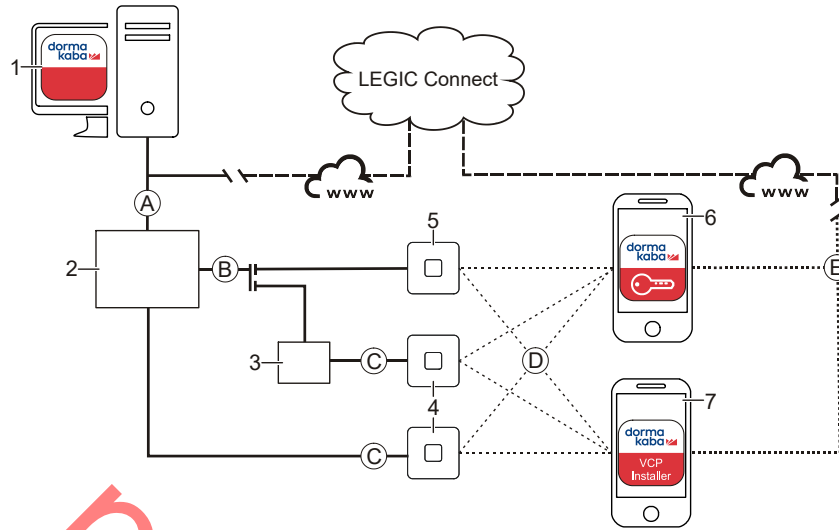
- The communication with the system software can be encrypted.
- Optionally, an external tamper switch can be connected.

**Use**

- Door management for up to 16 doors
- Personal interlocks
- Lift control
- Arming intruder detection systems

### 3.3 Mobile Access system overview

The system software distributes the access permissions via **LEGIC Connect** to the smartphones.



A	Ethernet	D	NFC or Bluetooth
B	RS-485	E	WLAN/mobile data
C	Coaxial cable/HF RFID		

1	System software	
2	Access manager	

		NFC	Bluetooth		NFC	Bluetooth	
3	<b>Remote reader</b>			5	<b>compact reader</b>		
	91 15 -K5	●	-		91 04 -K5	●	-
	91 25 -K5	●	-		91 04 -K6	●	●
4	<b>Registration unit</b>			91 10 -K5	●	-	
	90 00 -K5	●	-	91 12 -K6	●	●	
	90 01 -K5	●	-				
	90 01 -K6	●	●				
	90 02 -K5	●	-				
	90 03 -K5	●	-				
	90 04 -K5	●	-				

		Operating system	NFC	Bluetooth
6	Smartphone with <b>dormakaba mobile access</b> app The Mobile Access bookings are carried out with it.	Android	●	●
		iOS	-	●
7	Smartphone with <b>VCP Installer</b> app The VCP Installer initialises the Mobile Access function.	Android	●	●
		iOS	-	-

● yes

- no

## 3.4 Technical data

### 3.4.1 Power supply



Only power supply units that fulfil the following requirements may be used for power supply: LPS (Limited Power Source) and SELV (Safety Extra Low Voltage) in accordance with IEC/EN/UL/CSA 60950-1 or ES1 and PS2 in accordance with IEC/EN/UL/CSA 62368-1.

- **Voltage:**
  - 10-34 V DC
  - 20-34 V DC, if more than 5 extension modules are connected
- **Power consumption**
  - 6,5 W
  - additionally per extension module 90 30: max. 3.5 W
  - additionally per extension module 90 31: max. 1.2 W
  - additionally, per reader to RS-232 port: max. 2.5 W

### 3.4.2 Data retention in case of power failure

The time, data and the configuration are retained without a power supply.

- Battery-backed real-time clock  
Battery type: CR2032

### 3.4.3 Interfaces

- **Ethernet**
  - 10/100 Mbit/s  
IEEE802.3 compatible, auto-sensing, auto MDI-X
  - Signalling the status via LEDs
- **RS-485**
  - KCP protocol  
Transmission parameters: 19200 baud, 8 data bits, even parity, 1 stop bit
  - DP1 protocol  
Transmission parameters: 2,400/4,800/9,600/19,200/38,400 baud, 8 data bits, even parity, 1 stop bit
  - phgCrypt protocol  
Transmission parameters: 9,600/19,200 baud, 8 data bits, no parity, 1 stop bit
- **RS-232 A/RS-232 B**
  - Output voltage: 5 V DC, maximum 500 mA
  - Transfer parameters (default): 9600 baud, 8 data bits, even parity, 1 stop bit
- **Ant. A/ant. B**
  - For connecting registration units
  - Impedance of the coaxial cable: 50 Ω

### 3.4.4 Frequency bands and transmission power

- **RFID:** 13,56 MHz, 76,39 dBµA/m
- **NFC:** 13,56 MHz, 76,39 dBµA/m

### 3.4.5 Inputs

- **IN 1 - IN 4**  
and extension module 90 31 IN1-IN8
  - For connecting insulated switches
  - Integrated power supply: 5 V DC
  - Signalling the status via LEDs
- **Tamper**
  - For connecting insulated switches
  - Integrated power supply: 5 V DC

### 3.4.6 Outputs

- **OUT 1 - OUT 3**  
and extension module 90 30 OUT1-OUT8
  - Potential free switching contact
  - Maximum load current: 30 V AC/DC; max. 2 A

Power supply units must meet the following requirements.  
LPS and SELV as per IEC/EN/UL/CSA 60950-1 or ES1 and PS2 as per IEC/EN/UL/CSA 62368-1.

  - Signalling the status via LEDs

### 3.4.7 Terminals

- **Conductor type:** single-wire/multi-wire
- **Conductor cross-section:** 0.08–1.5 mm<sup>2</sup>, AWG 28–16
- **Insulation stripping length:** 6 mm

### 3.4.8 Environmental conditions

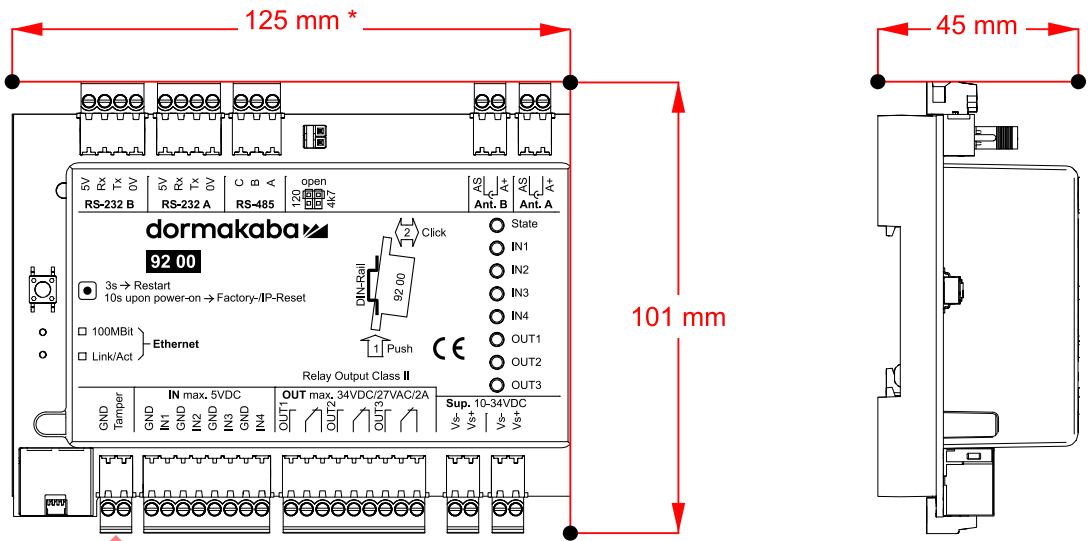
- **Class of protection:** IP20, as per IEC 60529
- **Relative humidity:** 5% - 85%, non condensing
- **Temperature**
  - Storage: -20 °C - +65 °C
  - Operation: -0 °C - +50 °C

### 3.4.9 Mechanics

- **Installation**
  - Top hat rails as per EN 60715: TH35/(7.5/15)
- **Weight**
  - 180 g

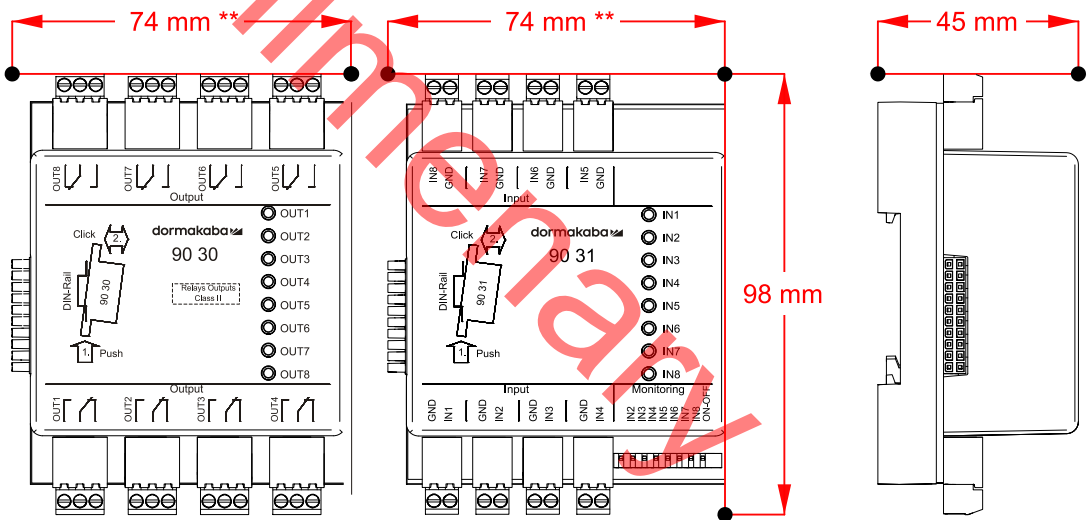
### 3.4.10 Dimensions

#### Access manager 92 00



\* corresponds to 7 horizontal pitches

#### Extension module 90 30/90 31



\*\* corresponds to 4 horizontal pitches

## 3.5 Conformity



This product complies with the standards

**EN 300330 V2.1.1**

**EN 301489-1 V2.2.0**

**EN 301489-3 V2.1.1**

**EN 50364:2010**

**EN 62368-1:2014-08**

in accordance with the regulations of the EU Directive

**2014/53/EU – Radio Equipment Directive (RED)**

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



You can download the original declaration of conformity in PDF format at [www.dormakaba.com/conformity](http://www.dormakaba.com/conformity).

**UL/CSA** This product complies with the following standards.

- **UL62368-1:2014-12**
- **CAN/CSA-22.2 No. 62368-1:2014-12**

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

**FCC ID NVI-DKAM9200-K7**

**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.

**IC** **Industry Canada Radio Standards Specifications RSS-GEN Issue 5, Sections 8.8, 8.9 and 8.10 and RSS-210 Issue 10, Section A2.6 (Category I Equipment)**

**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**

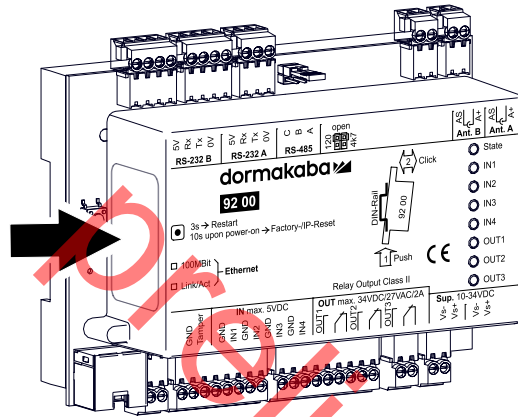
This device complies with Industry Canada’s licence-exempt RSSs. Operation is subject to the following two conditions:

- (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.

### 3.6 Identification



#### Identification label

The following can be found on the identification label:

- Manufacturer’s address
- Product code, function type
- Connection data of power supply
- Article number
- Hardware version
- Production date
- Protection type
- CE marking, optional additional conformity marks
- Note: Disposal as household waste is prohibited

## 3.7 Open source information

The firmware contains packages that are subject to open source licenses.

dormakaba provides the following legal information for each firmware version.

- List of open source packages
  - Name and version of the packages
  - Name and version of the licenses
- Detailed information on the individual packages
  - Detailed license texts
  - Information on copyright

The legal information can be accessed via the following.

- dormakaba extranet
  - The firmware and the legal information are packed in a ZIP file.
- Accessing the device via browser/console program

### **Disclaimer**

In accordance with the conditions of the open source licenses, dormakaba points out that the developers of packages have excluded any liability and warranty for the packages and their properties. The details are available in the respective license conditions.

By pointing out this exclusion of liability, dormakaba exclusively fulfils the license conditions of the packages. Legal and contractual claims against dormakaba are not affected by this exclusion of liability.

Provisional



### 3.8 Included in supplied package

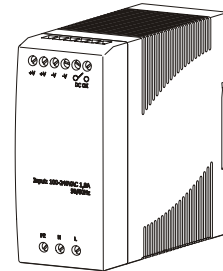
- 1 x Access Manager 92 00
- 1 x Quick start guide

### 3.9 Accessories

#### 3.9.1 Top hat rail power supply units

The installation must be carried out by qualified electricians.

The power supply unit is fitted on a top hat rail TH35/(7.5/15).



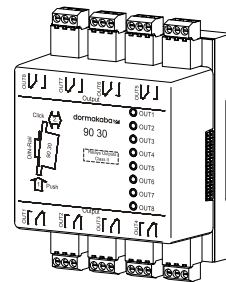
Input voltage	Output voltage	Output	Order code
100-240 V AC	12 V DC	60 W	04045052
100-240 V AC	24 V DC	60 W	04043074

#### 3.9.2 Extension module 90 30

The module features eight additional outputs.

The extension module is fitted on a top hat rail TH35/(7.5/15).

Order code: 04044693

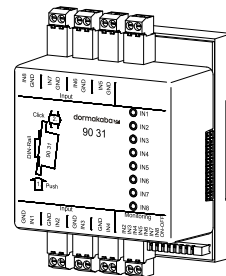


#### 3.9.3 Extension module 90 31

The module features eight additional inputs.

The extension module is fitted on a top hat rail TH35/(7.5/15).

Order code: 04044699



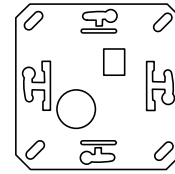
### 3.9.4 Detection units

#### Registration unit 90 00

Class of protection: -

Installation: On-site switch or socket ranges

For order code, see catalogue



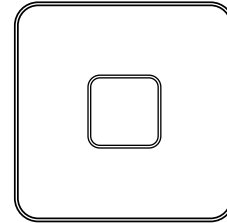
#### Registration unit 90 01

Colour: black or white

Class of protection: IP40 or IP54

Cable feed: Surface-mounted or flush-mounted

For order code, see catalogue



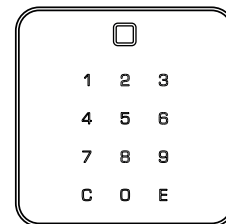
#### Registration unit 90 02

Colour: black or white

Class of protection: IP40 or IP54

Cable feed: Surface-mounted or flush-mounted

For order code, see catalogue



#### Registration unit 90 03

Colour: Black

Class of protection: IP55

Cable feed: Flush-mounted

For order code, see catalogue



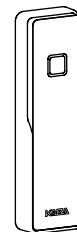
#### Registration unit 90 04

Colour: black or white

Class of protection: IP66

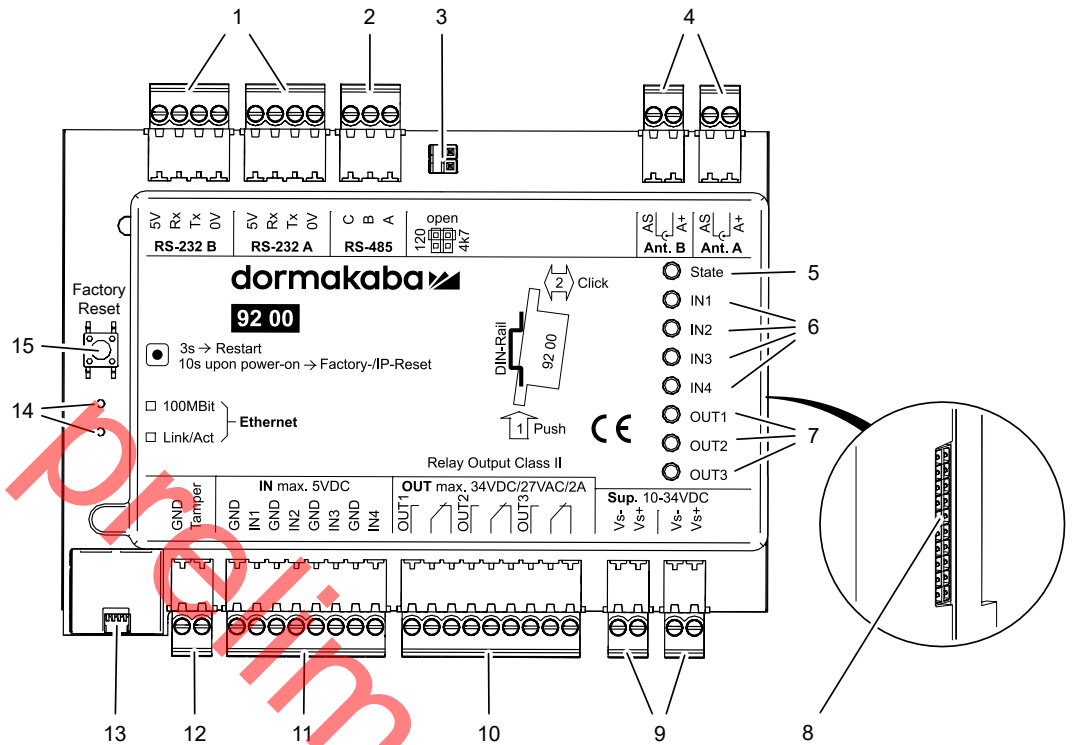
Cables: Length 8 m or 30 m

For order code, see catalogue



# 4 Construction and function

## 4.1 Device layout



- 1 RS-232 ports A + B
- 2 RS-485 port for connecting readers
- 3 Jumper for RS-485 bus connection
- 4 Connections for registration units
- 5 Status LED
- 6 IN-LEDs
- 7 OUT-LEDs
- 8 Connection for extension modules
- 9 Connection for the power supply
- 10 Outputs
- 11 Inputs
- 12 Input for connecting a tamper switch
- 13 Ethernet port
- 14 Ethernet LEDs
- 15 Reset button

## 4.2 Signal

### 4.2.1 Device status

The status LED indicates the device's status.

Signalling on start-up of system:

1.	2.	3.	4.	5.	6.	7.	08.
Solid red light	Off	Flashing red	Solid yellow light	Solid green light	Off	Solid green light	Flashing

System start	Operation
--------------	-----------

Signals during operation:

Status LED	Meaning
Off	No power supply
Flashing green (*)	The device is ready for operation.
Flashing red (*)	An IP address is assigned to the device.

(\*) The flashing frequency indicates the load of the CPU of the device. The slower the status LED flashes, the more the CPU is loaded.

At normal load, the status LED flashes once a second.

Indication when pressing the reset button, see:

- Restart reader [▶ 7.1](#)
- Reset the device to factory settings [▶ 7.2](#)

### 4.2.2 Ethernet LEDs

The LEDs next to the Ethernet connection signal the Ethernet port status.

Designation	Status	Explanation
100 MBit/s	Off	Transmission rate = 10 MBit/s
	Shines	Transmission rate = 100 MBit/s
Link	Off	No connection
	Shines	Physical connection to the network active

### 4.2.3 IN/OUT LEDs

The LEDs signal the states of the inputs and outputs.

Designation	Status	Meaning
IN1-IN4	Off	Input is not active (open)
	Solid green light	Input is active (closed)
OUT1-OUT3	Off	Output is not active
	Solid green light	Output is active (relay is energised)

## 4.3 Reading behaviour

### 4.3.1 Behaviour with two registration units

The access manager communicates alternately via the connections "Ant. A" and "Ant. B" (toggle) with the registration units connected to it. Hence, the access manager cannot communicate with both registration units at the same time. This results in the following behaviour:

- During a longer read process, the respective other registration unit is blocked.
- The fields of the two connected registration units do not influence each other. Therefore, the two registration units can be installed close to each other.
- In case of such registration units installed close to each other, it may happen that the medium is read by both registration units in succession.

### 4.3.2 Behaviour of readers installed next to each other

Readers which are installed next to each other do not influence each other during the read process.

Minimum distance between two readers: approx. 30 cm

### 4.3.3 Behaviour when several media are present in the field (anti-collision)

Several RFID user media (prime, ISO14443A and ISO15693) can be detected in the field simultaneously. Only the first user medium that corresponds to the search criteria defined in the system is considered.

## 4.4 System requirements

Function	Access manager firmware	System software
	<ul style="list-style-type: none"> <li>• TP4 client</li> </ul>	<ul style="list-style-type: none"> <li>• MATRIX Professional</li> <li>• MATRIX ONE</li> </ul>
General	≥ Version 4.00	≥ Version 3.2.x
Mobile Access	≥ Version 4.00	≥ Version 3.2.x <ul style="list-style-type: none"> <li>• MATRIX Professional                             <ul style="list-style-type: none"> <li>– with option E320 Mobile Access</li> </ul> </li> </ul>

### 4.4.1 Mobile Access system requirement

- |                 |   |
|-----------------|---|
| General         | <ul style="list-style-type: none"> <li>• The access control system is set up by dormakaba for Legic Connect</li> </ul>  |
| System software | <ul style="list-style-type: none"> <li>• See the chapter System requirements</li> <li>• A connection has been set up to Legic connect</li> </ul>  |
| Reader          | <ul style="list-style-type: none"> <li>• The reader supports Mobile Access.</li> <li>• The reader is configured in the system software for Mobile Access.</li> <li>• The configuration is transferred.</li> <li>• The reader is installed and ready for operation.</li> </ul> |

Also see

- Mobile Access System Overview chapter
- Planning guideline, Mobile Access

# 5 Installation

## 5.1 Installation requirements

### 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 location

The product is designed for the stationary use in buildings. The product is not suitable for the use in vehicles.

The access manager is mounted on a top hat rail in a housing or IT rack.

The access manager should be installed in a location where it is safe from tampering within the area being secured.

The mounted height for the terminal should not be higher than 2 meters.

#### **Electromagnetic fields**

Do not install the device in the vicinity of strong electromagnetic fields caused, for example, by switched-mode power supplies, electric power lines, phase control etc.

### 5.1.3 Connections

The following connections must be present at the installation location:

- Ethernet cable, with RJ45 plug
- Power supply cable
- Lines to electric strikes and contacts
- Lines to the RS-485 devices
- Coaxial line to the detection units

## 5.2 Installation lines

### 5.2.1 General requirements

The installation of the cables must conform to the current national and local regulations. In general, the following requirements apply.

- Protection against manipulation
  - Install the cables inside the security areas.
  - Install the cables so that they are hidden or difficult to access.
- Avoiding malfunctions
  - Keep the cable routes short.
  - Lay low-voltage and data lines away from sources of interference.

### 5.2.2 Ethernet

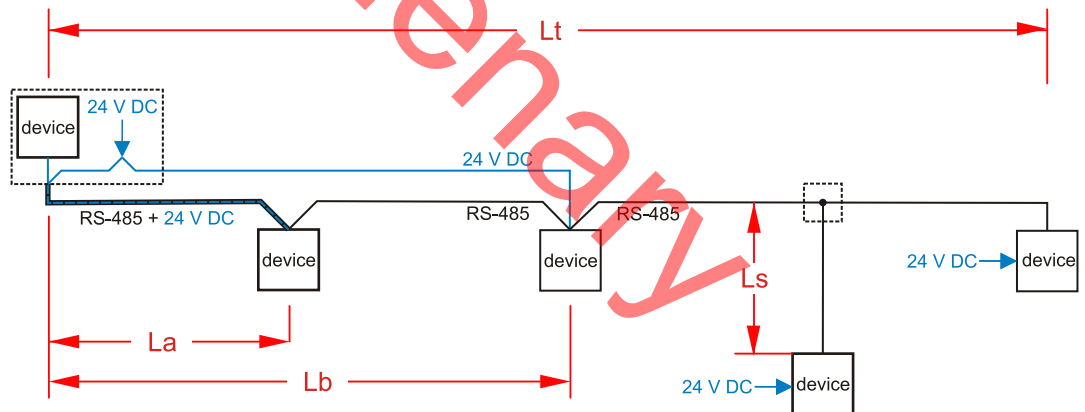
Network cable with RJ45 plug, line requirement: CAT.5 S-UTP 4 x 2 AWG 24 oder AWG 22 (according to EIA/TIA568) or higher quality.

### 5.2.3 Lines to RS-485 devices

The RS-485 devices are connected via a bus in 2-wire technology.

#### Wiring requirements

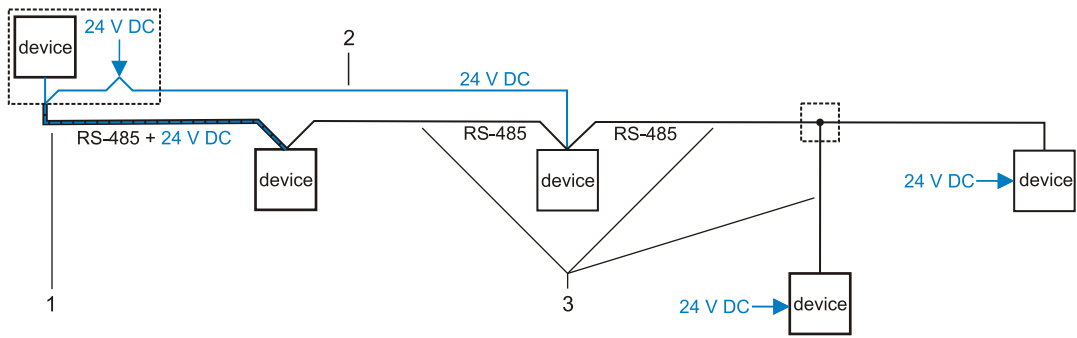
- Shielded line with twisted wire pairs.
- No other signals may be carried in the wire, except for the low voltage for the power supply to the RS-485 devices.
- Cable lengths:



<b>L<sub>t</sub></b>	The total permissible length (master and branch lines) is max. 1200 m.
<b>L<sub>a</sub></b>	If the RS-485 bus and the extra-low voltage is led through one cable, the max. permissible length is 20 m. <ul style="list-style-type: none"> <li>• If the distance is long, lay a separate line for the low voltage.</li> </ul>
<b>L<sub>b</sub></b>	Low voltage in a separate cable <ul style="list-style-type: none"> <li>• The length depends on the voltage drop of the cable. The voltage must conform to the requirement of the RS-485 device.</li> <li>• For longer distances, use a local power supply.</li> </ul>
<b>L<sub>s</sub></b>	The permissible length per branch line is max. 100 m. <ul style="list-style-type: none"> <li>• Not recommended, since branch lines can cause malfunctions.</li> </ul>

**Recommended cabling**

For the RS-485 bus, use only cables of the same type.



1	CAT.5 S/UTP 4x2 AWG 22 or J-Y(ST)Y 2x2x0.6
2	J-Y(ST)Y 2x1x0.8
3	CAT.5 S/UTP 4x2 AWG 24 or J-Y(ST)Y 2x1x0.6

**5.2.4 Line to the door opener, the door opener key, and the 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.

**5.2.5 Coaxial cables to registration units**

Registration units are connected to the access manager via coaxial cables. The coaxial cable transfers the HF signals from the RFID antenna, keyboard data and trigger data for the optical and acoustic signal generators.

Line requirements: Coaxial cable 50 ohms, type RG174/U.

Maximum cable length: 30 m

Recommended cable length: < 10 m

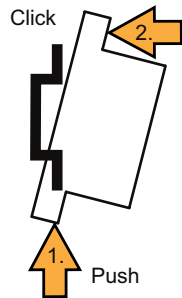


### 5.3 Mounting device and extension modules

Mount the devices on a 35 mm DIN rail (BS EN 60715).

**Prerequisites**

- The top hat rail is installed and grounded.



**Procedure**

1. Without tilting it, attach the device to the bottom of the DIN rail, press up and keep pressing it.
2. At the same time, push the device up against the DIN rail until it can be mounted on the DIN rail.

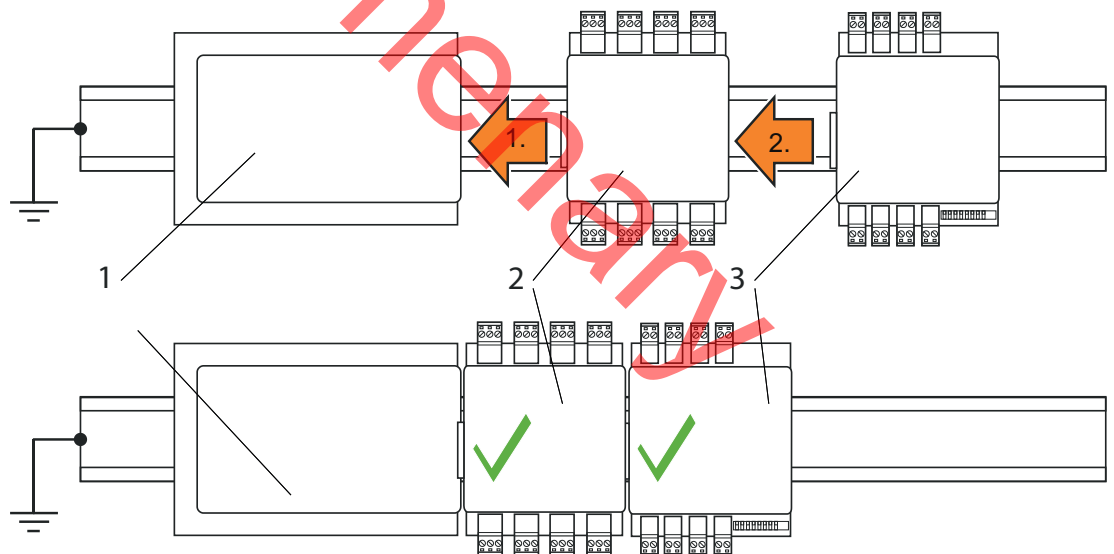
**Connect the extension modules**



**NOTICE**

**Attaching extension modules under voltage may cause damage to the devices.**

Before attaching the extension modules, switch off the power supply to the device!



- 1 Access manager 92 00
- 2 Extension module 90 30
- 3 Extension module 90 31

1. First plug in all extension modules 90 30 carefully to the device (1) or to an extension module 90 30 (push devices together on the DIN rail).
  - ⇒ All extension modules 90 30 are plugged in.
2. Then plug in the extension modules 90 31.
  - ⇒ The extension module 90 31 which is closer to the device (1) is detected as **Module 1**. The next is detected as **Module 2**.

- Secure the device and the extension module with 2 end clamps (safety clips) to avoid slipping.

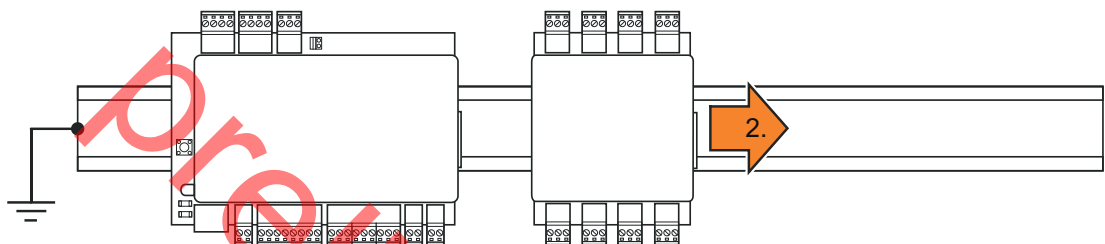
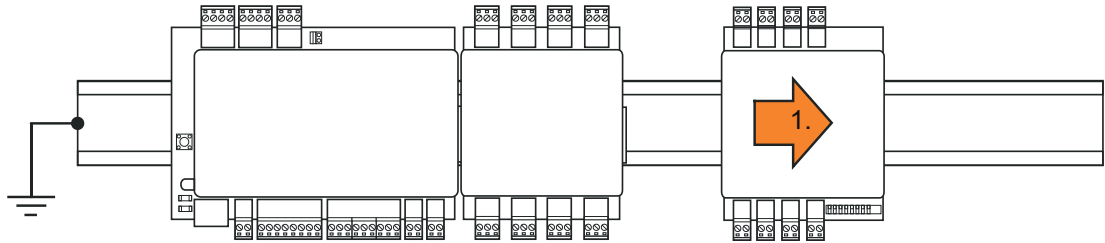
**Removing the extension modules**



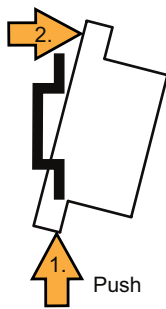
**NOTICE**

**Removing extension modules under voltage may cause damage to the devices.**

Before removing the extension modules, switch off the power supply to the device!



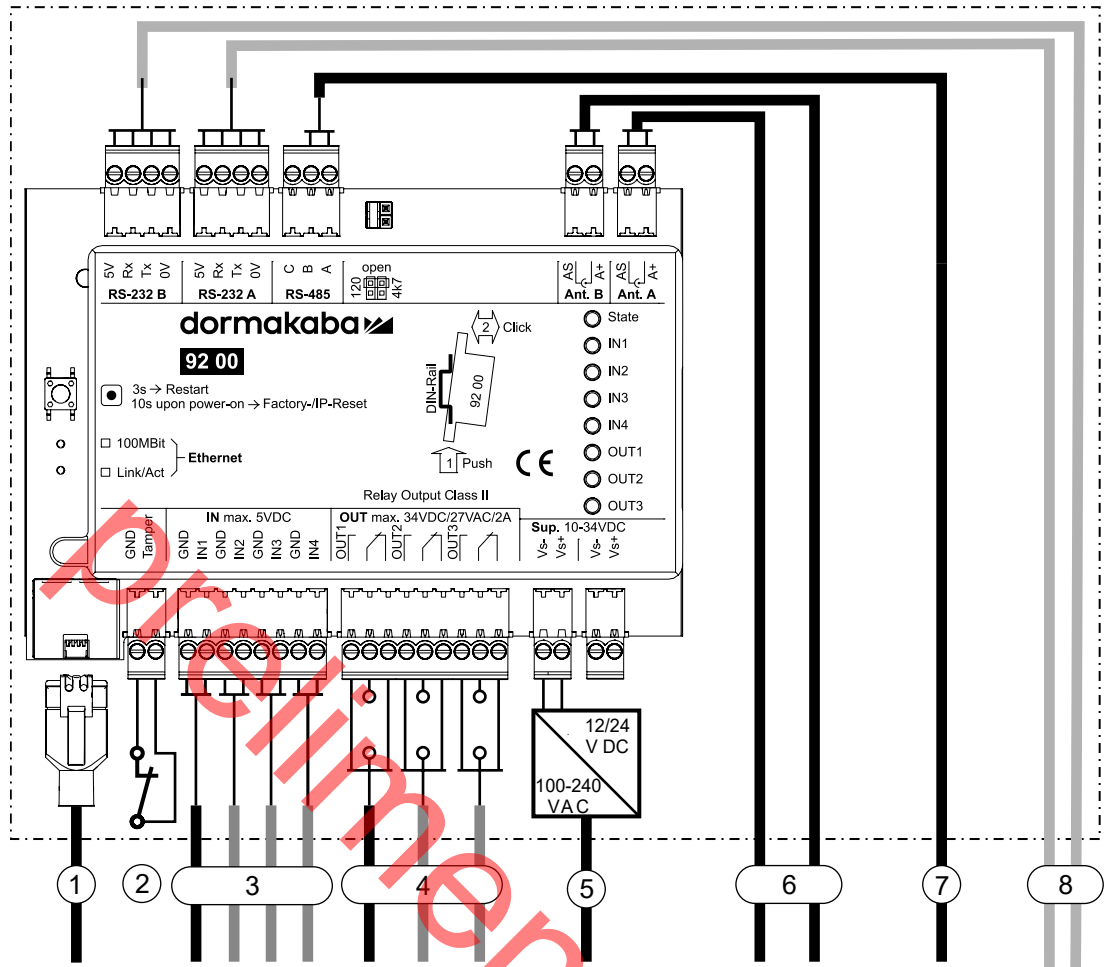
- Push the extension module away from the neighbouring module until there is no more contact.
- Remove the separated extension module from the DIN rail.



Preliminary

## 5.4 Connections

### 5.4.1 Overview



Connection	Connection for
Ethernet [1]	Network
Tamper [2]	Tamper switch
IN1 - IN4 [3] (Inputs)	Sensors  Example: Electric strike button, door handle, door frame, deadbolt, passage contact, other...
OUT1 - OUT3 [4] (Outputs)	Locking device/signal transmitter  Beispiel: Electric strike, motor lock, turnstile drive, other...
Sup. 10-34VDC [5]	Power supply
Ant. A / Ant. B [6]	Registration units
RS-485 [7]	Readers and other RS-485 devices
RS-232 A / RS-232 B [8]	Barcode scanner/reader

## 5.4.2 Power supply



### ⚠ WARNING

#### Live connections in the top hat rail power supply unit section

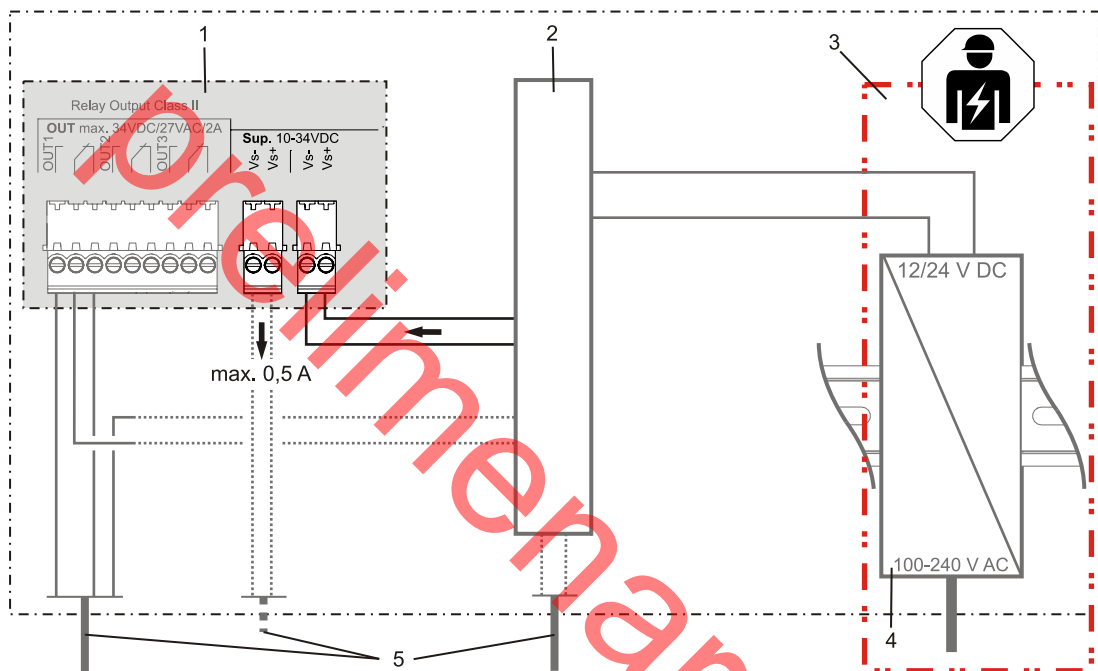
Carelessness can lead to an electric shock.

- Only electrical technicians should have access to the installation section with the power supply units to power the device.



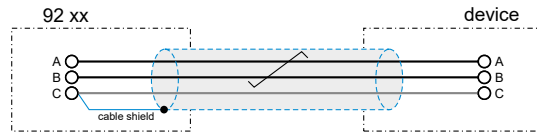
Only power supply units that fulfil the following requirements may be used for power supply: LPS (Limited Power Source) and SELV (Safety Extra Low Voltage) in accordance with IEC/EN/UL/CSA 60950-1 or ES1 and PS2 in accordance with IEC/EN/UL/CSA 62368-1.

There are two ports for the power supply. The ports are connected in parallel. The power supply is provided via one port. The second port can be used for supplying additional devices.



- 1 Device
- 2 Power distribution
- 3 Installation area only for qualified electricians
- 4 Top hat rail power supply unit
- 5 additional devices (reader, electric strike, ...)

### 5.4.3 RS-485 port

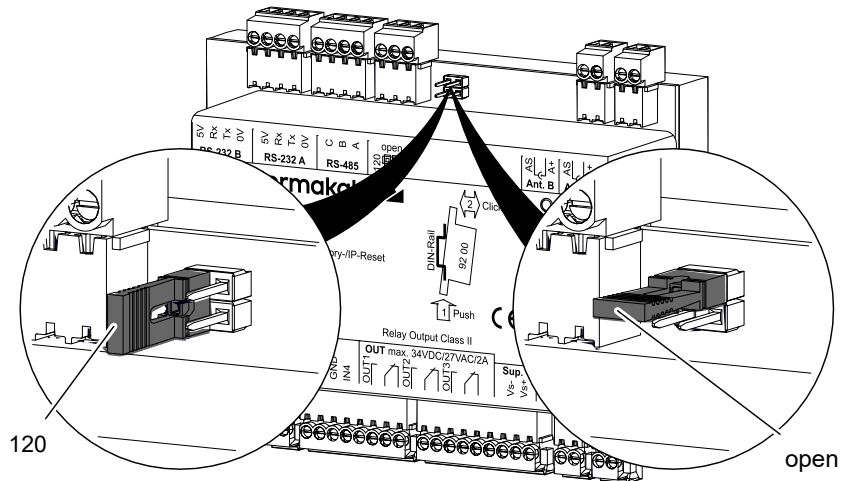


#### Connection diagram

- A ↔ A; B ↔ B
- optional C ↔ C
- Connect the cable shield on one side of the terminal C of the access manager.

preliminary

### 5.4.3.1 Terminal resistance



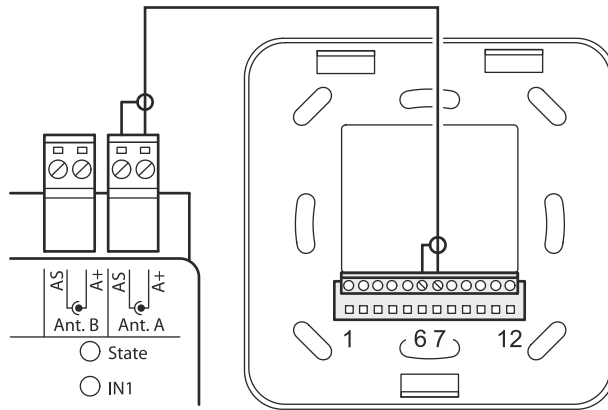
Set the terminal resistance with the jumper. The jumper must be plugged in at a valid position.

Jumper Position	Use
120	<ul style="list-style-type: none"> <li><b>Bus wiring</b> The device (1) is connected at the end of bus.  </li> <li><b>Star wiring</b>  </li> </ul>
open	<ul style="list-style-type: none"> <li><b>Bus wiring</b> The device (1) is connected within the bus.  </li> </ul>

- |   |                        |      |                             |
|---|------------------------|------|-----------------------------|
| 1 | This device            | 120  | Terminal resistance 120 Ω   |
| 2 | Additional bus devices | open | without terminal resistance |
|   |                        | 4k7  | Terminal resistance 4.7 kΩ  |

### 5.4.4 Registration units

The registration units are connected to the terminals labelled **Ant. A** and **Ant. B**.

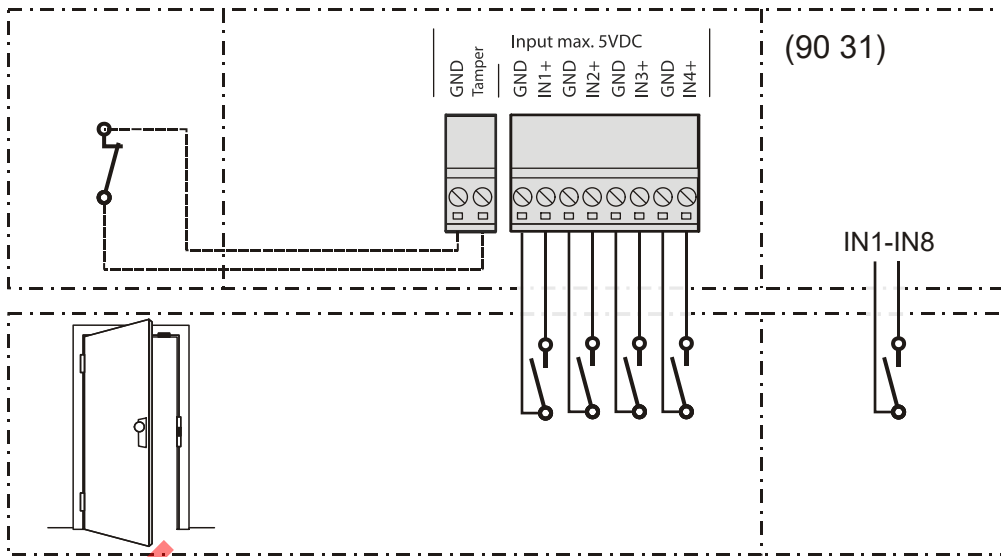


Connection identification	Assignment
A+	Coaxial cable neutral conductor
AS	Coaxial cable shield

Preliminary

### 5.4.5 Inputs

Each input has two contacts (IN+, GND). One input is activated by closing the two contacts.



The inputs on Extension Module 90 31 all operate in the same way.

The inputs can be assigned different functions. Assignment of the functions is done by the system software.

Frequently used functions:

Function	Contact	Status
Electric strike button	open:	Standby mode
	closed:	Electric strike button activated
Door frame contact	open:	Door open
	closed:	Door closed
Bolt contact	open:	Door unlocked
	closed:	Door locked
Passage contact	open:	Standby mode
	closed:	Access event complete
Door handle contact	open:	Standby mode
	closed:	Handle used
Tamper switch (Tamper)	open:	Tamper alarm
	closed:	Standby mode

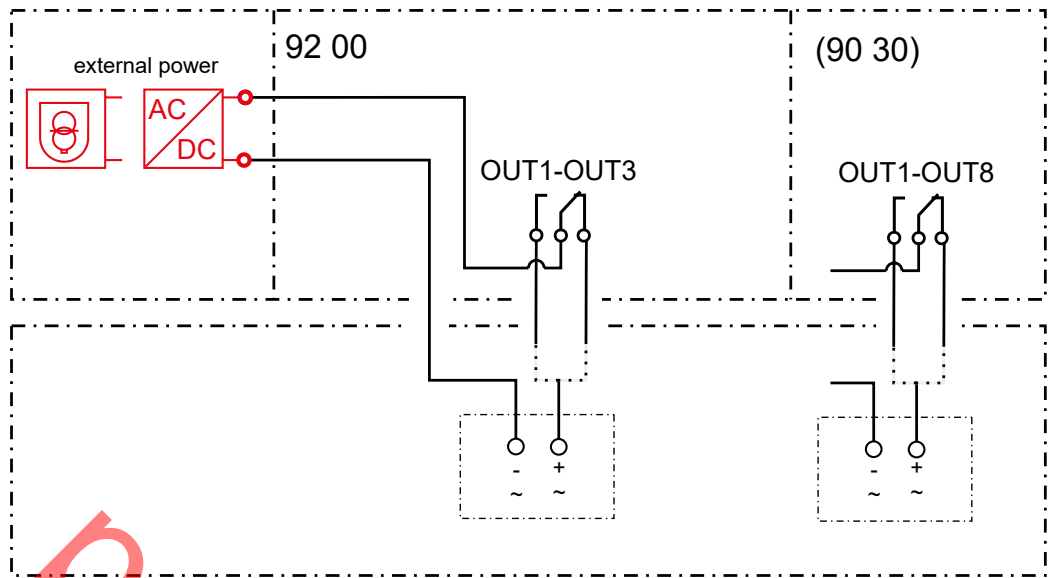


The statuses described correspond to standard settings. The system software can also carry out a reverse interpretation of the statuses.



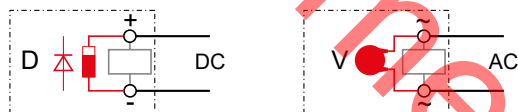
### 5.4.6 Outputs

Each output consists of a change-over contact.



If an inductive appliance (relay, electric strike, ...) does not have separate interference suppression measure, the following interference suppression measure must be attached to the appliance:

- Direct current (DC): Connect a diode [D] parallel to blocking direction.
- Alternate current (AC): Connect a varistor [V] parallel.



[D] Type: 1N4004; [V] Type: S10K30

External power supply units are required for the power supply

- Maximum load current: 30 V AC/DC; max. 2 A

Power supply units must meet the following requirements.

LPS and SELV as per IEC/EN/UL/CSA 60950-1 or ES1 and PS2 as per IEC/EN/UL/CSA 62368-1.






The outputs on Extension Module 90 30 all operate in the same way.

# 6 Commissioning

## 6.1 Network parameters

Agree on the network parameters of the network, the device and the system software, and set them.

Overview of the ports		Setting		
Designation	Number			
<ul style="list-style-type: none"> <li>• <b>Server command</b> (TCP) for data transfer from the device to the system software</li> </ul>	Standard: 3000 Range: 1–32,767	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• <b>Terminal command</b> (TCP) for data transfer from the system software to the device</li> </ul>	Standard: 3001 Range: 1000–32,765	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• <b>ITM</b> (TCP) Inter-terminal communication</li> </ul>	= <i>Terminal command +1</i>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• <b>Network monitoring</b> (TCP) Network monitoring of units among each other</li> </ul>	= <i>Terminal command +2</i>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• <b>Telnet</b> (TCP) Access to service functions via Telnet.</li> </ul>	Standard: 23 Range: 1–32,767	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• <b>mDNS</b> (UDP) Multicast DNS</li> </ul>	5353 (fix)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• <b>DNS</b> (TCP/UDP) Host name resolution by DNS server</li> </ul>	53 (fixed)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• <b>HTTP/HTTPS</b> (TCP) You can use a browser to open a configurable transaction page via the web server</li> </ul>	Standard: 80/443 Range: 1–32,767	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• <b>SNMP</b> (UDP) To monitor the LAN interface with SNMP</li> </ul>	Standard: 161 Range: 1–161	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Setting**



Network: Firewall

The required ports must be released and activated.

- required
- needed for MATRIX Device Scanner, otherwise optional
- optional



Device: Supplied state

- On
- Off

The following ports can be activated/deactivated in the system software.

- Telnet
- HTTP/HTTPS
- SNMP

Other settings:

- Ports=Standard
- DHCP operation: on
- Host name = '<MAC-Adresse>.local'. The MAC address is input without the ':'.



System software

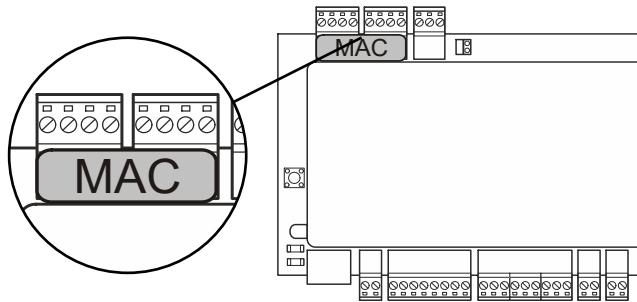
- Optionally encrypted communication can be activated.
- Encryption not possible.

The IP address or the host name must be input in the system software.

Preliminary

## 6.1.1 MAC address of the device

The MAC address can be found on a label.



The host name in the delivered state is = '<MAC-address>.local'. The MAC address is input without the ':'.  

---



**Recommended:**

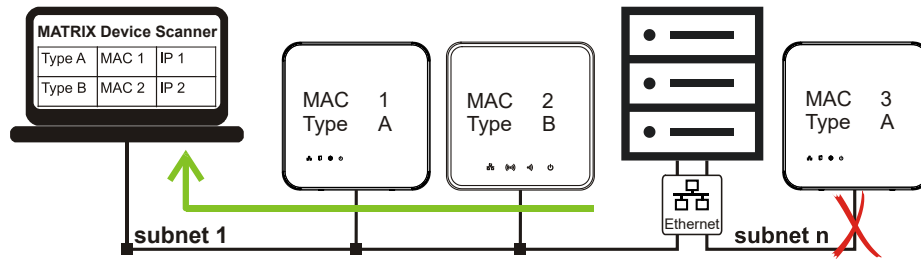
Note the device's MAC address. The device can be uniquely identified in the network based on the MAC address.  

---

preliminary

## 6.1.2 Change network parameters with 'MATRIX Device Scanner'

The program 'MATRIX Device Scanner' finds dormakaba devices with an Ethernet interface on a network.



### Prerequisites

- The necessary ports are activated on the network.
- The devices are installed and available.
- The devices can be found in the same subnet.
- Microsoft Windows compatible laptop
  - LAN interface
  - Network setting:
    - Automatically get IP address (DHCP on)
    - Automatic private IP address (APIPA)
 With this setting, devices are found on networks without a DHCP server.

**Functions** The program offers the following functions.

- The network parameters of the devices can be set for the initial setup.
  - Use DHCP
  - Assign static IP (IP address, network mask, gateway IP)
- The IP addresses of the devices are discoverable.

**Installation** The program must be installed on a laptop. The installer can be found on the MATRIX DVD in the folder 'MATRIX Device Scanner'.

**Illustration** After program start-up, dormakaba devices are searched for on the network. The devices found are listed.

Columns				
Type	MAC address	IP address	Action	Comment

Column	Explanation
Type	The type of the devices
MAC address	The MAC address of the devices <b>Note:</b> The MAC address can be found on a label on the devices.
IP address	The current IP address of the devices
Action	<ul style="list-style-type: none"> <li>• <b>Empty field</b> The network parameters are set.</li> <li>• <b>Change network setting...</b> The network parameters must be set.</li> </ul>
Comment	<ul style="list-style-type: none"> <li>• <b>Empty field</b> The network parameters must be set.</li> </ul>

- **Device is already in use (...)**  
The network parameters are set.
    - (Device number ##) MATRIX device number
    - (Telnet not available)
    - (Password changed) only wireless gateway
- 

**Operation**   **Change the network parameters of the device**

- ✓ The device cannot be configured by MATRIX.  
**Alternatively:** Reset the device to factory settings.
- ✓ The MAC address is known.
  1. Search for the device on the list. (MAC address, type)
  2. Click the 'Change network settings...' button.
    - ⇒ A new window opens.
  3. Set the network parameters
  4. Click the 'Change settings' button.
    - ⇒ This window closes.
- ⇒ The network parameters of the device have been changed.

Preliminary

## 6.2 Configuration

The configuration of the device is done in the system software.

### Requirements

- The necessary ports are activated on the network.
- The system software is installed and ready for operation.
- The device is installed and ready for operation.
- The network parameters of the device are set for the existing network.
- The IP address or the host name of the device is known.

In the system software, carry out the following steps. A login as user with administrator rights is necessary.

1. Create and configure the device
2. Transfer the configuration data
3. Define access permissions for the doors
4. Define access permissions for persons

In existing systems, all the steps do not have to be carried out.

Preliminary

## 6.3 Initialise the device for Mobile Access



**See also:**

- Mobile Access system overview [▶ 3.3]
- Planning guideline, Mobile Access

Initialisation depends on the readers used.

Reader	Initialisation
Registration unit	The access manager is initialised via a registration unit.
Compact reader	Every compact reader must be initialised.
Remote reader	Every remote reader must be initialised via a registration unit.

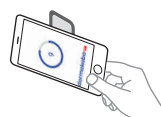
**Prerequisites**

- General
  - The access control system is set up by dormakaba for Legic Connect
- System software
  - See the chapter System requirements
  - A connection has been set up to Legic connect
- Reader
  - The reader supports Mobile Access.
  - The reader is configured in the system software for Mobile Access.
  - The configuration is transferred.
  - The reader is installed and ready for operation.
- Smartphone
  - The VCP Installer is installed and registered with the telephone number with Legic Connect. The registration code received via SMS is entered.
  - Access to the Internet is possible (WLAN or mobile data).
  - The password for the VCP file is known.

**Procedure**

- On the smartphone:
  - Start the VCP Installer.
  - Ensure that the method of transmission of the smartphone and the device is identical. Select the transmission type NFC or Bluetooth.
  - Select the VCP file.  
If the desired VCP file is not present, select 'Update'. Then, the smartphone downloads the VCP file.
  - Select 'Send'.
  - Input the password for the VCP file.
  - Transmission type:

**NFC**



Hold the smartphone in front of the reader.

**Bluetooth**



Keep the smartphone within Bluetooth range of the device.

If a device other than the one desired flashes: In the system software, match the 'RSSI filters' of the devices.



- Reader to which the smartphone is held:
  - After successful initialisation: Three signals are sounded.
  - After a **failed** initialisation: no signalling
  - Then, the device signals the base state defined in the parent system.
- Smartphone:
  - After successful initialisation: display of the serial number of the device.

preliminary

## 6.4 Additional steps for Legic media technology

With Legic media technology, a write/read authorisation is required in the following cases:

- If it is necessary to write to a write-protected segment of a medium.  
Example: AoC
- If a read-protected segment of a medium is to be read.

### 6.4.1 Grant read/write authorisation

The authorisation is granted via a registration unit.



The term "Write authorisation" is used in this chapter for the terms "Write authorisation" and "Read authorisation".

A write authorisation with a LEGIC prime SAM 63 card is only valid for LEGIC prime.

A write authorisation with a LEGIC advant SAM 63 card is valid for LEGIC prime and LEGIC advant 15693 and 14443A.

In this chapter, the names "Security card C2" are used for the card names "SAM 63" and "Security card C2 (SC-C2)".

#### Requirements

- A security card C2 with the corresponding segment zone is present.
- The ISO standard 14443A must have been activated with the security card C2.
- The ISO standard of the SAM 63 card must conform to the parameterised ISO standard.
- The device is in normal operation and waits for a RFID input.

#### Procedure

1. Hold the security card C2 in the RFID field until the signalling takes place
  - ⇒ Signalling after successful write authorisation:  
3x beep  
glows red till the next booking takes place
  - ⇒ Signalling after **unsuccessful** write authorisation:  
- "Access not authorised"

#### Possible reasons

- The security card C2 was removed too early from the RFID field.
- If no reaction: ISO 14443A is not activated in the system
- If using SAM+ media: there are no credits available

2. Remove the security card C2 from the RFID field.

## 6.4.2 Withdrawing read/write authorisation

Read/write authorisation must be withdrawn in the following cases:

- If no more data is to be written to write-protected segments of a medium.
- If reading from read-protected segments of a medium is no longer to be read.



In this chapter, the term 'write authorisation' shall be used to refer to both 'write authorisation' and 'read authorisation'.

### 6.4.2.1 Withdrawing all write access issued via a write authorisation

Reset the device to factory settings. (See chapter Maintenance)

### 6.4.2.2 Withdrawing individual write access issued via a write authorisation

The withdrawal is carried out via a registration unit.

#### Requirements

- For cancelling the write authorisation, a SAM 64 card with the corresponding segment zone is required.
- The device and the registration unit are ready for operation.

#### Procedure

1. Present the master medium.
  - ⇒ A brief signal sounds and glows green briefly.
2. Present the SAM 64 card uninterrupted to the compact reader (approx. 15 s).
  - ⇒ The registration unit glows green during the process.
  - ⇒ 3x beeps: Write authorisation was cancelled

If write authorisation has already been revoked before with the same SAM 64 card, this is signalled immediately with three beeps.

- ⇒ No signal: Write authorisation has **not** been revoked.

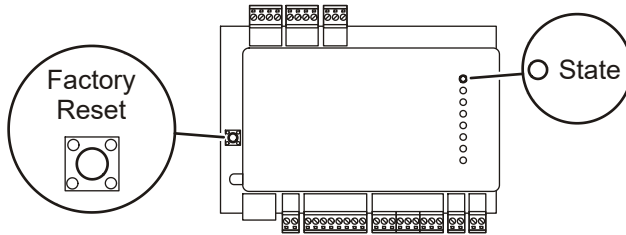
#### Possible reasons

- The SAM 64 card was removed from the RFID field too early
- ISO 14443A is not activated in the system
- If using SAM+ media: there are no credits available

3. Remove the SAM 64 card from the field.

# 7 Maintenance

## 7.1 Restart reader



The Reset button carries the name 'Factory-Reset'.

- Procedure**
- ✓ The device is ready for operation.
  - 1. Press the Reset button and hold it down.
  - 2. Release the Reset button as soon as the status LED glows red.
  - ⇒ The device restarts.

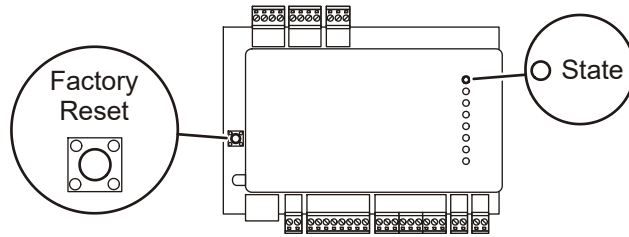
**Signal** Signal 'Restart device':

Time (s)	Status LED	Status upon releasing the Reset button
1	Solid yellow light	The Reset button is pressed.
2		• No effect
3		
4	Solid red light	The device starts afresh.

**Also see about this**

[4.2.1 Device status \[▶ 26\]](#)

## 7.2 Reset the device to factory settings



The Reset button carries the name 'Factory-Reset'.

- Procedure** ✓ The voltage supply is switched off.
1. Press the Reset button and hold it down.
  2. Switch on the voltage supply.
    - ⇒ The status of the device is displayed. See the signal 'Reset the device to factory settings'
  3. Release the Reset button after 5 to 8 s. See the signal 'Reset the device to factory settings'

**Note:**

If the button is pressed for longer than 10 s, the booting process is aborted.

**Signal** Signal 'Reset the device to factory settings'

Time (s)	Status LED	Status upon releasing the Reset button
1	Flashing yellow light	The device boots up.
2		<ul style="list-style-type: none"> <li>• The configuration is retained.</li> </ul>
3		
4	Solid yellow light	The device boots up. <ul style="list-style-type: none"> <li>• The configuration is deleted.</li> </ul>
5	Flashing red	The device boots up.
6		<ul style="list-style-type: none"> <li>• The configuration is deleted.</li> </ul>
7		
8		
9		
10		
11	Solid yellow light	The booting process is aborted. <ul style="list-style-type: none"> <li>• The data are not deleted.</li> <li>• The device is not operational.</li> </ul> <p>The power supply must be switched off and on again.</p>

# 8 Decommissioning

## Usage

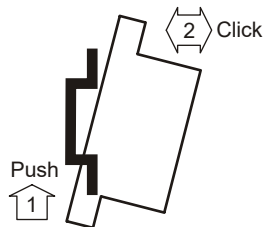
- The device is replaced with another device.
- The device is installed at another location.
- The device is disposed of.

## Procedure

- Delete the person-related data.
  - Reset the device to factory settings.
- In the parent system, set the device to inactive or delete.
- Maintain the changes in the system software.
- Switch off the power supply.

## 8.1 Dismantling

- ✓ The device was de-commissioned.
1. If present, unplug extension module
  2. Disconnect relay outputs from the device
  3. Disconnect inputs from the device
  4. Disconnect RS-232 interface/keyboards, biometrics or system-dependent functions from the device
  5. Disconnect detection units and readers from the device
  6. Disconnect device from the top hat rail



# 9 Packaging/return

Improperly packed assembly groups and devices may produce extra costs due to damage during transport.

Please observe the following instructions when sending dormakaba products.

dormakaba are not liable for damage to products which are due to inadequate packaging.

## 9.1 Complete devices

The original packaging is specially made for the device. It provides optimum protection against transport damage.



---

Always use the original packaging to return the device!

---

If this is not possible, you must provide packaging which will prevent any damage to the device.

- Use a sturdy, thick-walled transport case or a box. The transport case should be large enough to allow 8–10 cm clearance between the unit and container wall.
- Wrap device in a suitable foil or place in a bag.
- Pad heavily around the device with foam padding or air bags, for example. The device must not be able to move around within the packaging.
- Use dust-free, environmentally friendly fill material.

## 9.2 Electronic component assemblies



ESD-sensitive electronic component assemblies such as PCBs and readers should be stored, transported and shipped in suitable anti-static packaging. Electronic component assemblies must be packed at ESD-protected workstations. This should be carried out by persons who are familiar with and comply with general ESD protection regulations.

Electronic component assemblies must be returned in packaging with sufficient ESD protection to

- make warranty claims in the event of malfunctions of any type.
- Delivery of replacements for electronic PCBs and components in replacement procedure.

Electronic components shipped in packaging without adequate ESD protection will not be analysed or repaired to maintain a high quality standard; they will be taken directly for disposal instead.

## 9.3 Labelling

Including all returns paperwork and labelling the package correctly enables us to process your case quickly. Please ensure that a delivery note is enclosed in each package. The delivery note should contain the following information:

- Number of devices or components in each package.
- Article numbers, serial numbers, designations, order number.
- Address of your company/contact person.
- Reason for return, e.g. repair exchange.
- Accurate description of fault.

Returns from countries outside the EU also require a customs invoice with an accurate customs value and customs tariff number.

preliminary



# 10 Disposal



The device is indicated with the adjacent symbol which means prohibition of its disposal as household waste.

The device's integral components must be separated before they are taken for recycling or disposal. Old and used devices contain valuable recyclable materials which must be recycled. Toxic and hazardous components may cause long-term damage to the environment if you dispose of them incorrectly.

The facility operators are obliged to return electrical and electronic devices to their manufacturer, point of purchase or designated public collection points at the end of their service life.

Disposal in Germany:

dormakaba EAD GmbH will take responsibility for correct disposal of supplied goods once they are no longer in use as per statutory regulations (ElektroG in Germany). The owner of the used electrical appliance bears any costs incurred for transport to the manufacturer's plant.

Disposal in Switzerland:

The device is to be returned to an electrical appliance return point as per the Regulation on Returning, Taking Back and Disposing of Electrical and Electronic Equipment (VREG).

In the EU, electrical appliances should be taken for disposal in accordance with the country's respective disposal and environmental guidelines.

## Deletion of personal data

The owner/operator is responsible for deleting their personal data.



## Dispose of packaging in an environmentally responsible fashion.

The packaging materials are recyclable. Do not dispose of packaging in the household waste; take it to a recycling point instead.

# Index

<b>A</b>			
Access manager	16	iOS	16
Access on Card	8	IP class of protection	18
Ambient temperature	18	<b>K</b>	
AoC	8, 15, 48	KCP	8, 15
APIPA	8	<b>L</b>	
<b>B</b>		Legic Connect	27, 46
Basic safety instructions	10	LEGIC Connect	16
Bluetooth	8, 16	<b>M</b>	
booting process	51	MAC address	42, 43
<b>C</b>		Manufacturer	21
CE Conformity	20	Mobile Access	15
Class of protection	18	<b>N</b>	
Coaxial cable	30	Network cable	29
Configuration	45	network parameters	40
Conformity	20	NFC	8, 16
<b>D</b>		<b>P</b>	
Data on Card	8	Packaging	53
Data protection and IT security	15, 52	phgCrypt	15
Dimensional drawing	19	Product code	21
Dimensions	19	<b>R</b>	
Disposal	55	Radio Equipment Directive	20
DoC	8, 15	Registration unit	15
dormakaba mobile access App	16	Relative humidity	18
DP1	8, 15	Reset button	25, 50, 51
<b>E</b>		Return	53
Electromagnetic fields	28	RFID	8
ESD prevention measures	11	RFID-Technologie	15
Ethernet LEDs	26	RoHS	20
<b>F</b>		RS-232 port	25
Factory-Reset	50, 51	RS-485 port	25
firmware	27	<b>S</b>	
function type	21	Safety Instructions	10
<b>I</b>		Smartphone	16, 46
Identification label	21	Status LED	50, 51
Inductive appliance	39	Switching conditions	38
Installation lines	29	System software	16, 27, 45, 46
Interference suppression measure	39	Systemsoftware	15

**T**

Tamper switch	25
Temperature	18
TP4	8
TP4-Client	13

**V**

VCP	8
VCP file	46
VCP Installer	16
VCP Installer App	46

**W**

WEEE guideline	55
----------------	----

preliminary