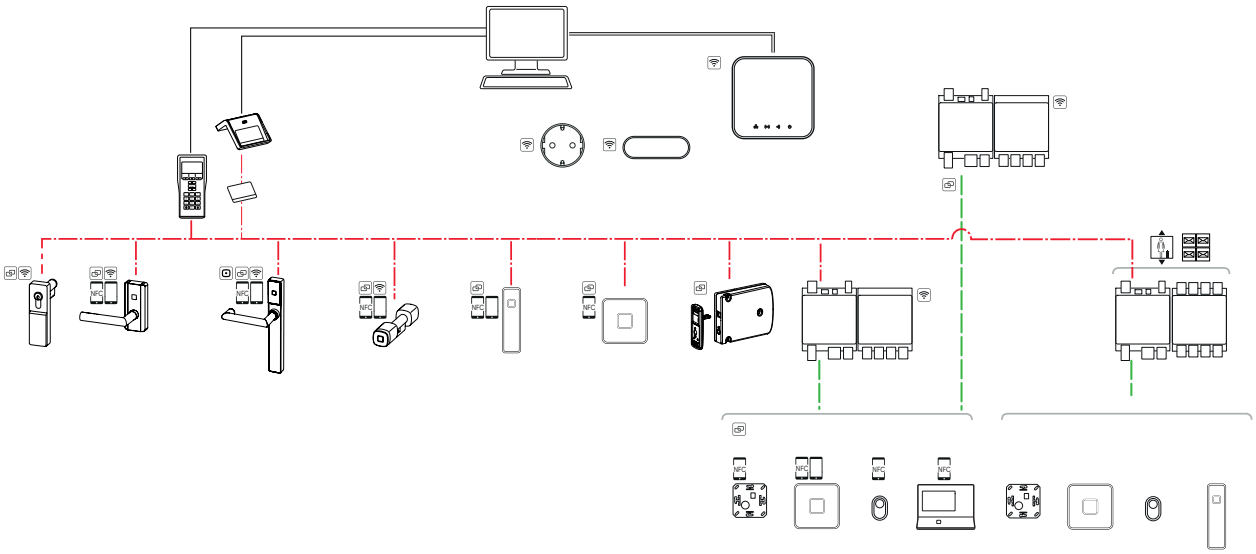
dormakaba

evolo Subsystem description

System description



Public - 11/2026

EN

Table of contents

1 About this document 5
1.1 New features and updates 5
1.2 Validity 5
1.3 Target group 5
1.4 Contents and purpose 6
1.5 Document availability 6
1.6 Additional documents 6
1.7 Abbreviations/definition of terms 6
1.8 Warnings 8

2 Overview 9
2.1 Authorization 9
2.2 Components 9
2.3 System software 11
2.3.1 Topologies 11
2.3.2 Tool chain 12
2.4 Smartphone access options 13
2.4.1 Mobile Access applications 13
2.4.2 Wallet-based access (Apple Wallet and Google Wallet) 14
2.5 Media 14
2.5.1 Master media 16
2.5.2 User media 17
2.6 Program structures 18
2.6.1 A/B and B structures 18
2.7 OSS-SO support 20

3 Authorisation types and functions 21
3.1 Identification number 21
3.2 System level 21
3.3 Whitelist authorisation 22
3.3.1 Whitelist authorisation with time profile 23
3.4 CardLink authorisation 25
3.4.1 Access rights 25
3.4.2 Validation 27
3.4.3 Validating media 27
3.4.4 Lost media 28
3.4.5 Blacklist 29
3.4.6 Service media 29
3.4.7 Status information 29
3.4.8 Media traceback 29
3.5 Access on Card 29
3.6 Mixed mode 30
3.7 Unauthorized media 30
3.8 TimePro functions 30
3.8.1 Office time profile 30
3.8.2 Day/Night time profile 32
3.9 Advanced functions 32
3.9.1 Wireless components 32
3.9.2 Component traceback 35
3.9.3 S-module 35
3.9.4 Escape return function for c-lever pro 35
3.9.5 Pass mode with c-lever pro 35
3.9.6 Pass-Lock with c-lever pro 36
3.9.7 Intervention media 36
3.9.8 Deactivating manual programming 36
3.10 TouchGo 37
3.10.1 RCID principle of operation 37
3.10.2 Security aspects 37
3.10.3 TouchGo E110 38
3.10.4 TouchGo E310 38

3.11 Free locker selection with cabinet lock 21 10 and 21 20 39
3.12 Letterbox/lift 39

4 System variants 40
4.1 Whitelist programming 40
4.1.1 Whitelist authorisation without tool chain 40
4.1.2 Whitelist authorisation with tool chain 41
4.2 CardLink programming 42
4.2.1 CardLink authorisation via desktop reader 42
4.2.2 CardLink authorisation via update reader 43
4.2.3 CardLink authorisation via terminal 44
4.3 Firmware variant overview 45

5 Security functions 47
5.1 LEGIC security levels 47
5.2 Security with CardLink authorisations LEGIC 47
5.3 Security with the whitelist authorisation LEGIC 47
5.4 MIFARE security levels 48
5.5 Security with CardLink authorisations MIFARE 48
5.6 Security with the whitelist authorisation MIFARE 49
5.7 Master T 50

6 Components 51
6.1 Memory sizes 51
6.2 Technical data 51
6.3 Master media 54
6.4 Security cards 54
6.5 Tool chain 55

7 Program/configure a component 57
7.1 Define media technology 57
7.2 Methods for programming and configuration 57
7.3 Programming TouchGo products 57
7.3.1 Programming TouchGo E310 57
7.3.2 Lost/defective user media 65
7.4 Programming with media 65
7.4.1 Cards 66
7.4.2 Key 72
7.4.3 INI reset with Master media 77
7.5 Programming with system software 79
7.5.1 System software for evolo components 80
7.5.2 Programming with system software and programmer 80
7.5.3 Export to components 80
7.5.4 Import from components 80
7.6 Mobile Access 81
7.6.1 System requirements 81
7.6.2 Initialising the device for Mobile Access 82
7.6.3 Initializing the device for evolo smart 83
7.6.4 Set Bluetooth signal strength 83
7.7 Initializing of wireless components 83
7.8 Setting the properties and functions of a component 84
7.9 Reset (INI reset) 84
7.9.1 Overview of INI reset variants for components 85
7.10 Saving energy 85
7.10.1 Deactivate functions 86
7.10.2 'Object in Field' function 87

8 Signals 88
8.1 Signal duration 88
8.2 Access authorisations 88
8.3 Pass lock (c-lever) authorisations 88
8.4 Escape return and pass mode (c-lever) authorisations 89
8.5 Messages when using the security card C2 89
8.6 Programming messages 89

8.7 Wireless 90
8.8 Reset messages 91
8.9 Error and fault messages 92

9 System maintenance 93
9.1 Maintenance schedule 93
9.2 Battery life 93
9.3 Buffer time for changing the batteries 94
9.4 Opening if batteries become discharged 94
9.4.1 Temporary emergency opening medium 95
9.5 Configuration and traceback 95
9.6 Firmware update for components 96
9.7 dormakaba ACS Service Tool 96

1 About this document

1.1 New features and updates

The following table contains the improvements in this version of the subsystem, its related components or software/firmware.

Change	Description	Intro-duced in
Passlock activation delay	A configurable delay can be set to prevent unintended activation of Passlock. The button must be held for the full configured duration before Passlock activates. See section Pass-Lock with c-lever pro [▶ 3.9.6].	42.48
Intervention media	A dedicated group of intervention media can be defined to retain access when Passlock is active, or when an intrusion detection system (IDS) is armed. See Intervention media [▶ 3.9.7].	42.48
Google Wallet support	Google Wallet can be used as user media via NFC on supported evolo components. See section Wallet-based access (Apple Wallet and Google Wallet) [▶ 2.4.2].	42.48
Apple Wallet support	Apple Wallet can be used as user media via NFC on supported evolo components. See section Wallet-based access (Apple Wallet and Google Wallet) [▶ 2.4.2].	42.46
Access on Card (AoC) option for unlimited validity	When using MATRIX, you can set unlimited access validity to a user when this is required by the business needs of the customer. See section Access on Card [▶ 3.5].	42.40
Wireless Gateway naming update	To reflect its latest improvements, this manual now describes the wireless gateway in its latest version **90 40-K7**.	-
c-lever air discontinued	The product is no longer offered to customers and is no longer mentioned in this manual.	-

1.2 Validity

The document describes the evolo subsystem for the RFID technologies LEGIC, MIFARE and MRD (Multi RFID Device). New systems use MRD technology.

The document describes the evolo subsystem for the use of Bluetooth® and NFC mobile technologies.

The description includes standalone, wireless, Bluetooth® and NFC components.

Firmware version installed on the components: version 42.38 and above

In this manual, descriptions or examples of how the components are used with host systems refer to usage with KEM. The procedure for integration of the evolo subsystem into host systems is described in the documentation of the respective host systems.

1.3 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

1.4 Contents and purpose

This document contains the basics of the evolo system and provides a collated overview.

1.5 Document availability

Supplementary documentation is available at the following link:

https://techdoc.dormakaba.com/cds

1.6 Additional documents

The following documents are available from the sales partners:

- Technical documentation of the components used
- Programmer 1460 manual
- Documentation for the system software used
- dormakaba evolo product catalogue

Touch Go option

- User manual for dormakaba c-lever pro TouchGo
- Planning guideline for dormakaba c-lever pro TouchGo with S-module

Wireless option

- Wireless planning guideline

Mobile Access option

- Mobile Access planning guidelines

1.7 Abbreviations/definition of terms

For readability, the following official product names are replaced with short names.

Product designation/definition	Short name
dormakaba evolo	evolo
dormakaba remote reader	Reader
dormakaba compact reader	
dormakaba digital cylinder	Digital cylinder
dormakaba mechatronic cylinder, surface-fixed	Mechatronic cylinder
dormakaba mechatronic cylinder, compact	
dormakaba mechatronic cylinder, forend	
dormakaba terminal 94 20	Terminal

Product designation/definition	Short name
dormakaba c-lever pro TouchGo	TouchGo
dormakaba c-lever pro	c-lever
dormakaba c-lever compact	
Kaba c-lever	
dormakaba cabinet lock 21 10	Cabinet lock
Wireless Gateway 90 40-K7	Wireless gateway
Wireless Extender 90 41	Extender
dormakaba remote reader 91 15 (E320) with wireless extension module 90 43	Wireless Reader
dormakaba desktop reader 91 08	Desktop reader
dormakaba Programmer 1364	Programmer 1364
dormakaba Programmer 1460	Programmer 1460
dormakaba evolo Manager	KEM
Kaba exos 9300	exos
dormakaba MATRIX ONE	MATRIX
dormakaba MATRIX PRO	
dormakaba b-com	b-com
Unique number	UID
Card identification number	CID
Radio frequency identification	RFID
Multi RFID device	MRD
CardLink®	CardLink
Access on Card	AoC
OSS Standard Offline	OSS-SO
Near Field Communication	NFC
Bluetooth®	Bluetooth
Bluetooth Low Energy®	BLE

The following symbols represent acoustic or visual signals:

Symbols		Signal type
		Acoustic signal
		Visual signal

There is no visual signalling for components without a visual display option.

1.8 Warnings

This manual contains information that you must observe for your own personal safety and to avoid material damage. The information regarding your personal safety is highlighted via a warning triangle; information regarding isolated material damage does not have a warning triangle. Depending on the hazard level, the warning information is displayed in decreasing order as follows:



⚠ 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.

The warning information for the highest level in each case is always used when several hazard levels occur at the same time. If warning information warns about personal injury, the same piece of warning information may also warn about material damage.

Other warning symbols:



General hazard



Risk of explosion



Danger from electric voltage



ESD: Danger from electrostatic discharge

Useful tips and information regarding safe operation of the product are labelled as follows:



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

2 Overview

The evolo subsystem is a set of standalone components whose configuration is transferred using the tool chain.

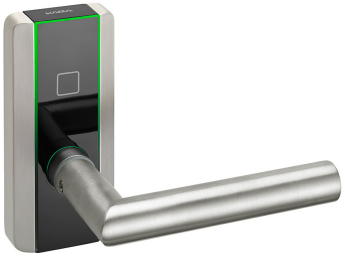
2.1 Authorization

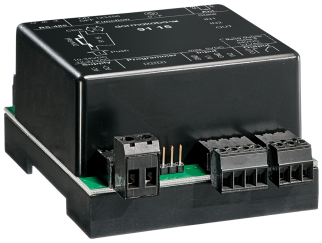
Description

Authorization	Description
Whitelist	The information regarding the authorization is present in the components.
CardLink	The information regarding the authorization is present in the user media.
Access on Card AoC	Only used under Matrix: The information regarding the authorization is present in the user media. Additional information on the AoC is given in the MATRIX documentation.
OSS-SO	Open standard. Additional information here: http://www.oss-association.com/standards/oss-standard-offline/
Mobile Access	With Mobile Access, smartphones become user media.

2.2 Components

Electronic components with miscellaneous functions that can be installed in or on doors.

	System overview of the components	
Product number	**Component**	**Description**
		c-lever pro **Options:** • Wireless • Mobile Access • OSS-SO • TouchGo E110 standalone only, not for evolo subsystems no wireless option • TouchGo E310 for evolo subsystems no wireless option
		c-lever compact **Options:** • Wireless • Mobile Access • OSS-SO

	System overview of the components	
Product number	**Component**	**Description**
143x / 153x		Digital cylinder **Options:** • Wireless • Mobile Access • OSS-SO
21 20		Cabinet lock • OSS-SO
91 15	 	Remote reader Device with remote registration unit **Optional extras:** • Wireless when used with extension module 90 43 (not shown) • Mobile Access (Bluetooth with corresponding registration unit) • OSS-SO • Paired with dormakaba compact reader sub-terminal 91 10

	System overview of the components	
Product number	**Component**	**Description**
91 04	 	Compact reader **Options:** • Mobile Access NFC only NFC and Bluetooth • OSS-SO • Paired with dormakaba compact reader sub-terminal 91 10
		Mechatronic cylinder **Options:** • Wireless • OSS-SO
		Letterbox access/lift control solution • Mobile Access

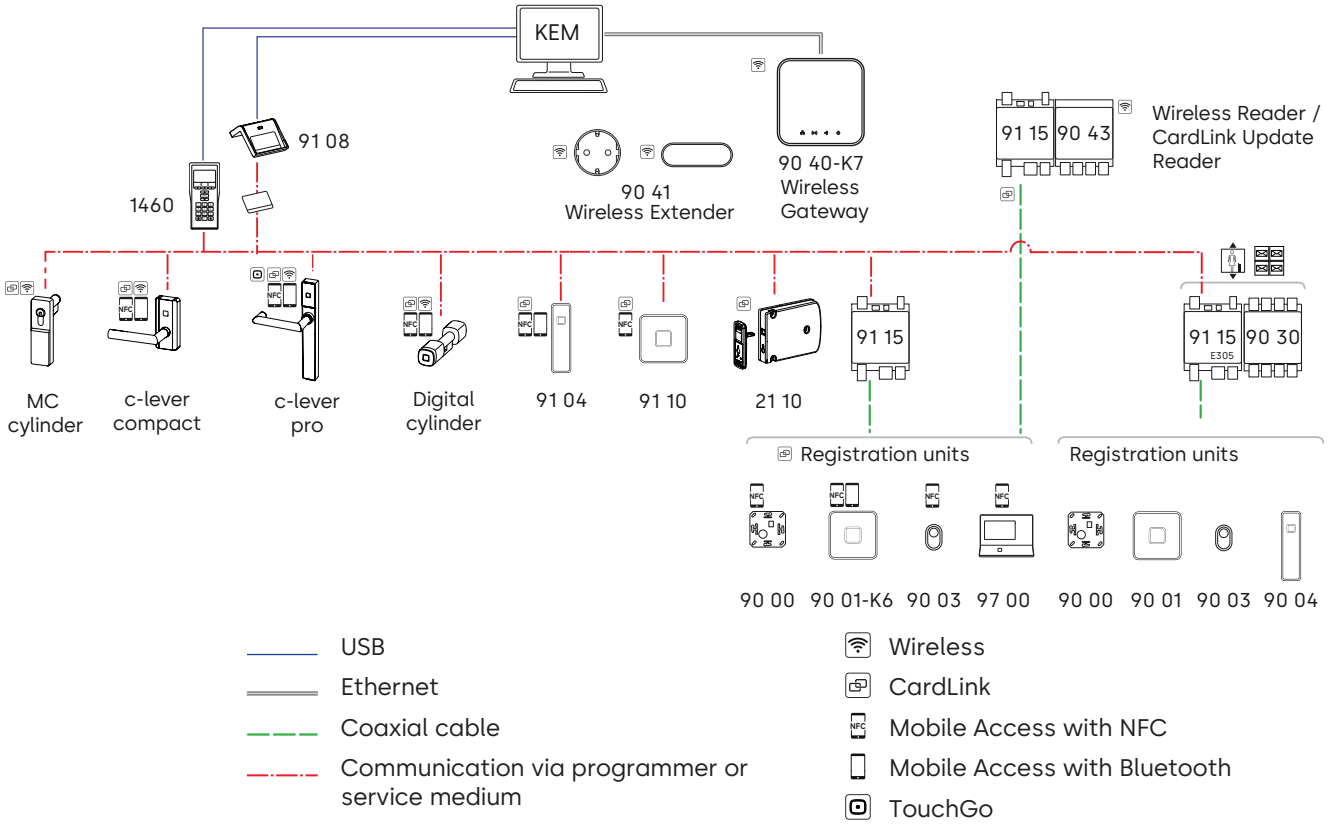
2.3 System software

evolo components can be configured not only with the dormakaba evolo Manager (KEM), but also with other system software.
Information on the possibilities is described in the documentation of the system software used.

2.3.1 Topologies

Example of a possible topology.

evolo components operating with KEM:
Edition: 03/2026



Legend				
90 00 90 01 90 03 90 04	Registration unit (Registration unit)		91 04 91 10	Compact reader
90 40-K7	Wireless gateway		91 15 91 25	Remote reader
90 41	Wireless extender		90 30 90 43	Extension module
1460	Programmer		91 08	Desktop reader B-web
91 15 + 90 30	Lift/letterbox control		91 15 + 90 43	Wireless reader Wireless CardLink update reader

The Wireless and Mobile Access planning guidelines provide more information on these topics.

Mobile Access with NFC: Mobile Access must be enabled in the component.
Mobile Access with Bluetooth: The component is equipped with the corresponding hardware for Bluetooth, and Mobile Access is enabled in the component.

See also Section [▶ 2.4.1]

2.3.2 Tool chain

System software and hardware for managing, reading and writing the authorization in components and media.

System overview of tool chain	
Tool	**Description**
	Desktop reader 91 08 MRD Media are read and written to with the system software and the desktop reader.

System overview of tool chain	
Tool	**Description**
	Programmer 1460 The device serves as the connecting link between the standalone components and the system software. The device is also used for the initial configuration/linking of wireless components to a wireless network.
	Wireless Gateway 90 40-K7 The device serves for linking wireless components to the system software.
	Wireless Extender 90 41 The device enlarges the range of the wireless gateway.
	Wireless Reader Wireless link for the remote reader 91 15 via a plugged-in wireless extension module 90 32. For CardLink update via wireless.
	Terminal For CardLink update

2.4 Smartphone access options

Users have the option to use mobile applications or wallet-based access as an alternative to their typical access media. Read the following sections for details.

2.4.1 Mobile Access applications

In Mobile Access use cases, access is achieved using the capabilities of a smartphone. With access permission, the lock/door can be opened manually. When access is granted, a visual and acoustic signal is emitted to notify the user.

Configuration parallel to conventional access with media is possible.

Technical requirement for full functionality:

In order to use Bluetooth, the component must be equipped with the appropriate hardware.

- Check the Bluetooth capabilities of the component using the programmer.

Technology	Smartphone Operating system	Peripheral
NFC	Android	Standard equipment and Mobile Access enabled
NFC + BLE	Android IOS	Bluetooth-enabled hardware and Mobile Access enabled

App	Description
mobile access app	Smartphone app for opening doors. User medium
VCP Installer	Smartphone app for putting door components into operation (evolo components, access readers).
evolo smart	Smartphone app for putting door components into operation and managing them. System software.

System software

The system software [▶ 2.3] is used to manage the key plan. In current versions, Mobile Access can be configured in the key plan. See section System requirements [▶ 7.6.1].

2.4.2 Wallet-based access (Apple Wallet and Google Wallet)

Apple Wallet and Google Wallet can be used as user media on supported evolo components. Access is granted to the user over NFC by holding the smartphone near the component. The dormakaba app is not required for this feature.

Wallet-based access is independent of the Bluetooth-based Mobile Access. No additional Mobile Access license is required, thus components from the E300 and E320 product lines are sufficient.

Requirements and restrictions

- The component firmware must be version 42.46 or higher (Apple Wallet) or 42.48 or higher (Google Wallet).
- If MIFARE media are used in the same installation, MIFARE DESFire is required. Wallet credentials are not compatible with MIFARE Classic.
- Host system support is required. Refer to the configuration documentation of the respective host system.

2.5 Media

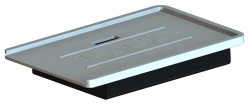
Master media do not have access authorizations.

System overview, media	
Medium	**Description**
Master media	
	Master A card Mechatronic cylinder Master A key
	Master B card Mechatronic cylinder Master B key
	Master T card (usage only with KEM)

System overview, media	
Medium	**Description**
	TouchGo master medium (RCID, only TouchGo E110)

The user media are used with their programmed access authorization on doors and in door groups.

System overview, media	
Medium	**Description**
User media	
	Card
	Card with QR code (evolo smart)
	Mechatronic cylinder
	Key fob
	Key fob with QR code (evolo smart)
	Mobile Access The access authorization is granted via smartphone. In different applications, configuration of the components via smartphone is also possible. See LINK [▶ 2.4.1] section: Mobile Access applications
	TouchGo key fob
	TouchGo wristband

System overview, media	
Medium	**Description**
	TouchGo card holder

Special media:

System overview, media	
Medium	**Description**
Security cards	
	The security card is created for every master key system and ensures site security. • MIFARE: Security card C • LEGIC: Security card C1 and C2
Wireless test medium	
	It is used, for example, for range measurement of wireless components. Only for wireless components. For more information, see the Wireless planning guidelines.
Licensing cards	
	System level upgrade Further information can be found in the System level section [▸ 3.2].

2.5.1 Master media

Master media are used to initiate or finish the programming process for standalone components.

No host system:

- After initiating the process, a manual whitelist is configured.
  See section "Programming with media".
- The Master Bs are organized under a Master A. Information about programming structures can be found in section "Programming structures".
- The master media do not have any access authorization.

With host system:

The documentation for the host system used contains information about the use of master media.

- After initiating the process, a configuration file is loaded using the programmer.
  See "Programming with system software".

Wireless components:

- A master medium is required to use the programmer to connect the device to the wireless gateway.

Master T:
Master T are temporary masters with limited validity and a limited range of functions. Master T are not available for all host systems. See the documentation for the host system used.

TouchGo:
The TouchGo E110 can only be programmed as a standalone whitelist and cannot be used with a host system. The RCID master is required for programming.

The TouchGo E310 can only be used in an evolo subsystem with a host system and tool chain. RCID and RFID authorization are configured in the system software and connected to the component via pairing. The master medium valid for the evolo subsystem is used.

Media



TouchGo



RCID, only TouchGo E110

2.5.2 User media

User media allow users to exercise the granted authorizations and to open doors, for example.

No host system
In whitelist programming, the user media are organized under a Master B.

NOTICE

Unauthorised access with lost medium

Remove lost medium from components:

- Revoke all access permissions with the Master (remove from the whitelist), see section "Revoke all access permissions assigned by Master B."
- Grant the still-valid user permissions (add to whitelist), see section "Grant access permissions."
- Repeat the process on all components to which the lost medium has access.

With host system
The access authorizations of the user media are programmed using configuration files. Information on this can be found in the section "Programming with system software" [▸ 7.5.2].

Media

RFID



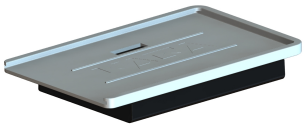


NFC/Bluetooth



TouchGo







User medium	RCID
Combi-medium	RCID + RFID

2.6 Program structures

Only for standalone programming without host system.
Whitelist programming only.

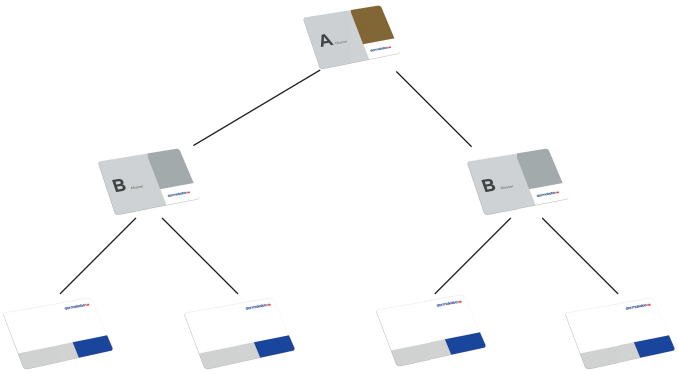
Components are organized in an A/B structure or in a B structure.

Programming is described in section "Programming with media".

2.6.1 A/B and B structures

Card-based systems:

A/B structure

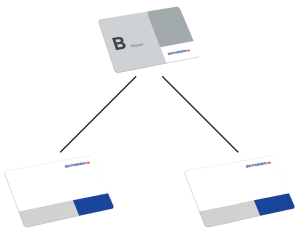


Master A

Master B

User media

B structure

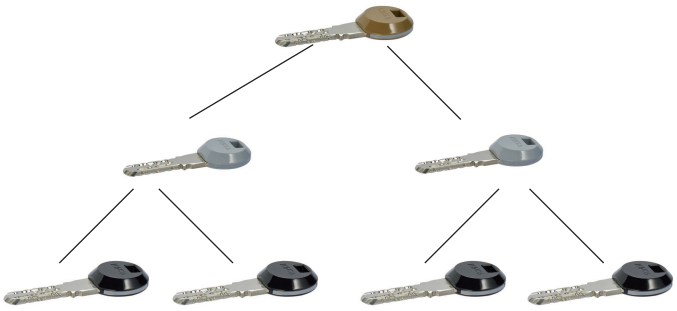


Master B

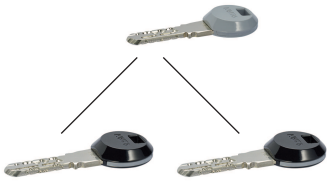
User media

Mechatronic systems:

A/B structure



B structure



Description/examples
A/B structure:

Master A:

- Create maximum 200 Master Bs
- No programming of the user media
- No programming of access authorizations
- For other applications, see the following chapter

Master B:

- Assignment and withdrawal of access authorizations

User media:

- Maximum 4,000 user media
- The distribution of the users over different Master Bs is at will

Example for one component of a site

- Master B1: 50 users
- Master B2: 3,950 users

Total = 4,000: Maximum number of users is reached.

B structure:

Master B:

- Assignment and withdrawal of access authorizations
- For other applications, see the following chapter

User media:

- Maximum 4,000 user media
- The distribution of the users across several Master Bs is **not** possible

Example for one component of a site

- Master B: 4,000 users

Total = 4,000: Maximum number of users is reached.

2.7 OSS-SO support

OSS-SO (Open Security Standards - Standard Offline) is an open industry standard for card-based offline access control. It enables interoperability between access control systems and offline locking devices from different manufacturers. Access authorisations are stored on the user medium (data on card) and are read directly by the component. The component does not need to be connected to the host system.

The evolo components can be used under OSS-SO. Configuration is performed using the OSS-SO toolchain and XML files supplied by the host system.

Limitations

The following functions are not supported when operating under OSS-SO:

- S-module switching functions S-module [▶ 3.9.3]
- Pass mode Pass mode with c-lever pro [▶ 3.9.5]
- Pass-Lock Pass-Lock with c-lever pro [▶ 3.9.6]

Mechatronic cylinder behaviour in office mode under OSS-SO

Office mode is not supported on the mechatronic cylinder. If the cylinder is part of an access group for which OSS-SO toggle permissions are configured, the component performs a normal opening instead of activating office mode. This behaviour is consistent with CardLink operation.

Additional information about OSS-SO:

- http://www.oss-association.com/standards/oss-standard-offline/
- Reference manual OSS-SO XML file
- OSS-SO toolchain user manual

3 Authorisation types and functions

The chapter describes the two authorization types whitelist and CardLink as well as the respective functions of the relevant evolo components.

- Whitelist: See section
- CardLink: See section
- AoC: See section [▶ 3.5]

3.1 Identification number

The media and the components are assigned an identification number for the authorization. It is required for unique identification.

The unique number (UID) is a unique identification number that is assigned by the card manufacturer and stored in the user media. It cannot be changed or deleted.

The Card ID (CID) is a unique identification number that is assigned via the system software. This is currently only possible with KEM. Media with defined CID can be ordered. The CID is stored with a one-off system key in the user medium and is read by the system components.

3.2 System level

The components are dispatched to the customer with a preset system level. The set system level determines the compatibility of the component with the host system used. The host systems provide the configuration for the system level assigned to them. This means that a component with a lower system level cannot be configured. A component with a higher system level can be used on a host system with a lower system level.

Overview
Overview of the host systems used and the matched system level.

System	System level	Definition on the Programmer
		Firmware from 1.30 onwards
evolo smart	SL1	1
MATRIX ONE / exivo / KEM	SL2	2
MATRIX PRO / exos / EACM	SL3	3
OSS (3rd Party + dormakaba host)	SL4	4

The system level of a component can be determined using the programmer.

Determining the system level status and “BLE ready”.
On the programmer, select the 'Actuator info' menu and read the information from the component.

Requirements:

- Programmer 1460
- Master medium of the component

Procedure:

1. Log in to the component with the master medium.
2. Select the 'Read actuator' menu.
3. Select the menu option 'Info'.
4. Connect the Programmer with the component.

Determine the firmware variant (E3xx) and version.

The system level is shown under SL.

Under BLE, a check mark shows that BLE is active.

The system level is supported by the components and host systems from the following versions.

The component can only be configured if the system level of the component and the configuration file are the same.
The component can be configured if the system level of the component is higher than the system level of the host system (Applies to SL1 to SL3. Does not apply to SL4).

A firmware update is also possible if the system level is incorrect.

Host system	from version	Remarks
exos	4.0.80	
KEM	5.3	
MATRIX	3.4	
evolo smart	2.0	
exivo		
EACM	7.6	
B-COMM	3.18.0	
Programmer 1460	1.26	The Programmer compares the system level of the parameter file with the system level of the component.
Component (firmware version)	42.28	In the factory, the system level is set according to the order.

Upgrade to a higher system level
The components are dispatched from the factory with the ordered system level. If certain functions are to be used, which are not released in that system level, then the system level of the component has to be updated as required. Upgrade media can be obtained for this purpose.



The following media are offered for upgrade/additional licences:

Upgrade	SL1 to SL2
Upgrade	SL2 to SL3
Upgrade	SL1 to SL3
Licensing	Mobile Access via BLE

The update procedure is described in the technical manual of the component.

3.3 Whitelist authorisation

A whitelist authorization is the set of the authorized media entered in the component.

The whitelist authorization is programmed in the components.
That is, the UID or the Card ID (CID) of the media to be authorized is stored in the component and thus, entered in the whitelist.
In the whitelist, the UID or the CID of the presented media is compared. If they match, the media are authorized and the components open. Up to 4,000 entries are possible in the whitelist. The UID or the CID can be entered.

Function example

Access authorisation will only be granted if user media are presented with UIDs or CIDs that are stored in the components.

Components	Media	Access
List of the UID stored in the components	**UID of the presented media**	
570AE209	570AE209	✓
222BE121	222BE121	✓
—	878EAE964	✗
—	121AC001	✗

3.3.1 Whitelist authorisation with time profile

Time profiles are used to define the times at which media are authorised at components.

All evolo components have their own (real-time) clock. This enables user media to be assigned time-related access authorisations for specific components and doors.

Alongside basic access authorisation, the time profiles enable time restrictions to be applied. The time profiles are specified in the system software.

3.3.1.1 Whitelist authorisation with individual time profile

Each component has a total of 15 freely definable time profiles available, each with 12 time windows.

3.3.1.2 Whitelist authorisation with unchangeable "Always" time profile

The status of this time profile is "Always" and it ensures that the door can be opened 24 hours a day, 7 days a week. The "Always" time profile cannot be changed, renamed or deleted.

3.3.1.3 Holidays/special days

Special days available:

Time profile V4	Features two special days A and B

Note: When components are updated with Programmer 1460, the system software always updates to the most current (today and in the future) holidays and special days.

Time profiles for holidays
Access authorisation can be issued or revoked for periods of sequential days (e.g. holidays). The length of a period can be defined by entering the start and end date. Several holiday blocks can be created. A total of 20 holiday blocks can be defined in the components (V4).

Note on the display of special days within holiday blocks: If there are special days within a holiday block, these are preferred in the display, i.e. the display of the special day is superimposed on that of the holiday block. If the special day is removed, the holiday block is displayed again in full.

Time window for special days
Two different days, special day A and special day B, can be created for special days (e.g. bank holidays). This makes it possible to create two time windows, e.g. one for the day before a bank holiday (special day A) and one for the bank holiday (special day B). For each of the two special day types, a total of 32 special days can be stored in the components.

Types of special days	Special day	Max. number of special days in the component
Special day A	Day before a bank holiday	32
Special day B	Bank holiday	32

3.3.1.4 Summer/winter time

Summer/winter time adjustments according to the global time zone setting are performed automatically in the components, depending on the set system software.

3.4 CardLink authorisation

With the authorization type CardLink, the access authorization is managed via the user media. In this manner, the local management work at the components is eliminated. The media applications on the user media are required for this type of authorization.
At the time of putting into operation, the components must be programmed once.

This authorization type also makes it possible to validate (activate for a certain period of time – Validation [▶ 3.4.2]) the user media for access authorization on the standalone components.

Advantages

- The access authorization is written directly to the user media.
- The authorization can be limited in terms of time in the function **Reservation**.
- A visitor can be assigned an individual selection of doors or door groups on a user medium.
- If there are additional user media, no further configuration is necessary on the components.
- Through the additional creation of groups, the structuring of the master key systems and the authorization assignment are simplified.

3.4.1 Access rights

A single, period limited authorization for a selection of components or door groups is assigned to the user media. To that end, a list of door groups or doors is stored in the user media.

Door group right
Door group rights can be combined organizationally (by persons) or spatially (by building sections).

A door group right is an access authorization with a parent time profile. For a door group right, several persons or doors are combined into a door group. The door group is stored in the components as identification and a time profile is assigned to the door group. Then, this door group can be assigned to the user media, which enables access to all the doors belonging to this door group.
For CardLink authorization, there are 15 time profiles with 12 time windows each available, as well as the time profile "Always", which is always valid. A corresponding time profile can be assigned to any door group.

Applications:

- For large master key systems with many users and doors. With the configuration of door groups, the master key system can be structured and managed with a clear overview.
- For a group of persons who are to get the same access authorization for a door group as that for group leaders and housekeeping services.

Individual right
An individual right is an access authorization with an individual time profile, which is valid for a single door or a door group.

The time profile of an individual right is stored on the user media. With an individual right, as against the door group (door group right), the time profile can be selected individually.

There are two variants available:

1 Individual right for single doors
For a door, user media can be assigned access authorization with individual time profiles.

2 Individual right for a door group
For a door group, individual users (their user media) can be assigned access authorization with individual time profiles.

Applications:

– For small master key systems with less users and doors.

– For several users, who are to be given individual access authorization to single doors, such as for cleaning staff and security forces.

– For individual users who are to get the individual access authorization for a door group, such as for group leaders and housekeeping services.

Reservation
A reservation is an access authorization for visitors, as with individual rights, but additionally with a start and end date or period of validity.

Applications:

- The reservation is a temporary authorization and is used for customers, visitors and suppliers.

Prioritization of rights
The rights have been prioritized. Through the prioritization of the rights, the access authorization of a medium can be restricted or expanded.

The rights are processed in the following sequence.

- Individual right
- Reservation
- Door group right

The evaluation of the following right is only continued if no “temporally incorrect” right is found. If a “temporally incorrect” right is found, the test is cancelled immediately.

However, searching is carried out within the evaluation of the door group right, until such time as:
a) all the rights have been examined or b) a valid right (door group and matched time profile) is found.

Function example

See below for a number of examples of different access rights.

Conditions are as follows:

- Door group A --> time profile 1
- Several components --> door group A
- "Entrance" door --> time profile 1 to 15

Example of access rights:

Access rights	Medium with data	Access for	
		Door group A	**Door "Input"**
Door group right	Door group A	✓ During time profile 1	✗
Individual right of door group A	Door group A + time profile 4	✓ During time profile 4	✗
Individual right of door	“Input” + time profile 3	✗	✓ During time profile 3
Reservation of door group A	Door group A + time profile 2 from start to stop	✓ During time profile 2 start to stop	✗

Access rights	Medium with data	Access for	
Reservation of door	"Input" + time profile 7 from start to stop	✗	✓ During time profile 7 start to stop
Combination between door group right and individual right	Door group A "Input" + time profile 3	✓ During time profile 1	✓ During time profile 3

3.4.2 Validation

Validation (time stamp on user media) is the activation of an access authorisation. Access is possible only with a valid CardLink authorisation and activated duration of validation [▶ 3.4.3].

Advantages

- Lost user media can be blocked quickly and easily by means of validation.
- CardLink authorisation expires once the duration of validation lapses. This means that the access authorisation and validation are deleted. Validation can no longer be renewed.

3.4.3 Validating media

Validation with standalone components

The standalone components can also be used as validation components. The validation components can be configured for the validation of CardLink authorization. If there is a modification to the validation, the components must be updated with Programmer 1460 or via wireless.

Since the validation needs additional energy, it is recommended to use only components for this purpose that have an external energy supply. For example, remote readers, compact readers or c-levers with an S-module are suitable.

Validation with Wireless Update Reader

User media can be validated on one or several wireless update readers. At the same time, the validation or the access authorization of lost user media can be withdrawn there. The validation data is managed by the system software and transferred to the update reader via wireless.

Validation with terminal

User media can be validated on one or several validation terminals. At the same time, the validation or the access authorization of lost user media can be withdrawn directly at a terminal. The terminal is managed from the system software.

Validation period

With the validation at a validation terminal or a validation component, a time stamp is written on the user media. From that time, the access authorization is valid for CardLink standalone components.

When user media are presented, the period of validity of the media is examined. That is, access is only granted if the period of validity has not expired and the temporal authorization for the corresponding door group or door (matching the time profile) is available.

The following validation types can be used:

Validation types	Status
Duration in days and hours	In days and hours. (Max. value 999 d and 24 h)
24 hours (1 day)	The type cannot be changed.
End time for the day (h)	Up to a certain time in the day.

Validation types	Status
"Always"	The type cannot be changed.

For the validation type "Always", lost user media cannot be disabled any more. Therefore, lost user media must obligatorily be entered for an unlimited time in the Blacklist [▶ 3.4.5] of the components.
The memory capacity for entering lost media in the blacklist is limited.
This validation type is not recommended for application.

Validation types
As regards the validation types, a distinction is made between media type and component type. The type of validation is always set at the component. Both validation types can be used in a master key system.

Media type (default)
The duration of the validation is created on all user media by default. When user media are presented to components, the current time stamp and validation duration of the user media are read and compared with the current time of the component. If the current time is earlier than the time stamp and the duration, the validation is valid. If the current time is later, the validation time is considered to have expired and the medium is invalid.

Component type
The duration of the validation is stored on the components. When user media are presented to components, only the current time stamp of the user media is read and compared with the current time of the components. If the time is within the validation period, the authorization of the user media is valid. If the time is later, the validation time is considered to have expired and the medium is invalid and not authorized any more.

The following validation types are possible:

Validation types	Validation period determined by	To be updated: Time stamp
Media (default)	Media	On the media
Components	Components	On the media

Function example
In a master key system, the validation period of 48 hours is selected, which is stored in the user media. With every entry at the main entrance, the user media are updated and granted access for the doors in the building. Employees who come in cars use the parking lot in the outdoor area, which is secured with a barrier. Since validation is not possible on the component of the barrier, the validations are not valid any more from 48 hours after the weekends or holidays. The barrier would remain closed. For this case, the barrier can be configured with the component validation. This makes it possible to set a validation period of four weeks. This ensures that the barrier opens even with a time stamp that is three weeks old.

3.4.4 Lost media

The validation is not renewed for lost user media. This makes these media invalid and access is blocked.

There are four options to exclude lost media:

- With terminals, the medium is set in the system software to the status "lost" and then no longer validated from the terminal.
- In the case of validation components, the medium is entered in the blacklist. The lost medium can no longer be validated. However, the medium only becomes invalid after the validation period has elapsed.
- In operations with standalone components, the medium is entered in the blacklist. Then, the data is transferred with the Programmer, or a service medium, or if present, via wireless to all the standalone components of the respective site.
- In operations with wireless components, after the lost medium has been annulled in the system software, a new parameter setting is transferred to the components.

3.4.5 Blacklist

Using the Blacklist function, user media can be blocked on all standalone (validation) components.

If user media have to be blocked within the period of validity of a validation, this blocking has to be performed with the Programmer 1460 or a service medium on all standalone components of the corresponding site. Then, the reverse confirmation can be transferred to the system software with Programmer 1460 or the respective service medium.

The blocking can also be performed via the tool chain system software -- Programmer or wirelessly.

3.4.6 Service media

Service media are only available under KEM.

Before media can be used as service media, they must be defined as such using the system software. Function cards, which are identifiable as such due to their unique layout, are available for this purpose.



User media that have been lost can be entered into the Blacklist [▶ 3.4.5] using the system software. This blacklist entry is written to the service medium and through it transferred to the components. Reconfirmation is performed by re-reading the service medium into the system software.

3.4.7 Status information

The status information is additional information that is transferred from the component to the media. If the battery charge level of a component drops too low, this status information is written to the media. When media with this status information are read by a desktop reader or a terminal, the information is passed on to the system software and displayed there.

With wireless components, the status information is transferred wirelessly to the system software and displayed there. If required, the process must be triggered in the system software.

3.4.8 Media traceback

The function can be configured in the system software.

In the CardLink authorization type, there is the option of saving media-specific access events on the user media. These data can be read by a desktop reader or terminal and transferred to the system software.

For example, the following events and statuses are stored:

- Access with authorization
- Access rejected
- Validation invalid
- incorrect time

3.5 Access on Card

When using the Access on Card (AoC) mode, the authorizations are saved in the user medium. The access data has a validity period that can vary depending on the user's needs. The validity period can also be set to be unlimited, that is, to not have an expiration date. The AoC mode is set in the MATRIX environment.

With Data on Card, data of the component are stored on the user medium when making a booking. These are read by a reader connected to a host system for further processing in the host system.

3.6 Mixed mode

In mixed mode, authorizations are saved on either a CardLink or a Whitelist medium. If the medium is held up to a component configured in mixed mode, the component first checks for a Whitelist authorization. If no authorization is found, a check is performed for CardLink authorization. The component opens if the medium is authorized in one of these authorization types.

If the medium is found in both authorization types but classified as "not authorized" in one of the authorization types, the medium is denied.

Example: The component does not open if there is a valid CardLink authorization for a medium but also a Whitelist authorization with a time profile outside of the validity.

3.7 Unauthorized media

The components remain closed when unauthorized user media are presented. If user media are presented in the open status, the components remain open. The components signal the rejection of unauthorized media.

3.8 TimePro functions

This chapter describes the TimePro functions Office and Day/Night.

Detailed supplementary information on both of the TimePro functions and their properties for the electronic components can be found in the KEM system software operating manual.

For c-lever and c-lever pro, the TimePro functions cannot be combined with the following functions:

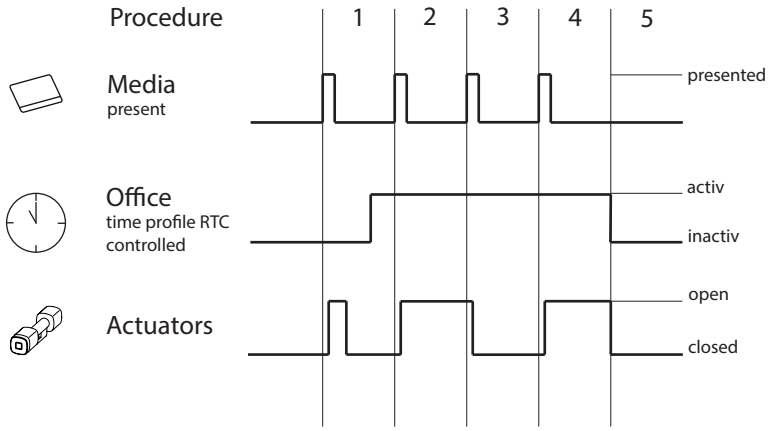
- Pass mode
- Escape return

3.8.1 Office time profile

Within the entered TimePro time profile, authorised media may change components to the open status.

Note: The Office time profile function can be restricted in the system software to individual user media.

Practical example



Procedure 1
The closed components are opened using authorised user media. After a certain open period (of a few seconds), the components close again automatically.

Procedure 2
Once authorised user media have been presented, the components remain permanently open.

Procedure 3
If authorised user media are presented when the components are in the open state, they will close again.

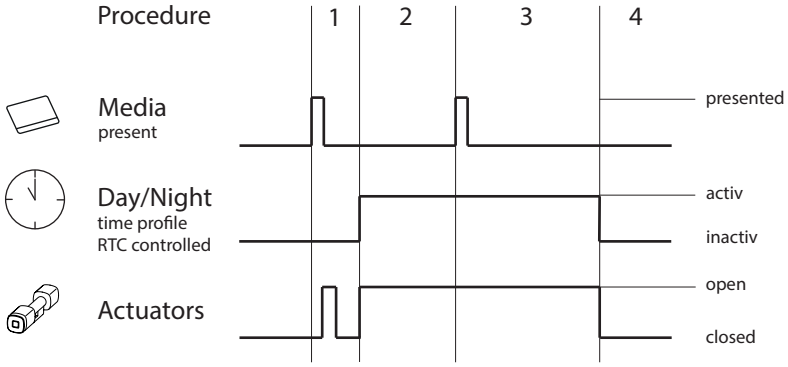
Procedure 4
After authorised user media are presented again, the components remain permanently open.

Procedure 5
If the Office time profile has expired, the components close automatically.

3.8.2 Day/Night time profile

The time profile Day/Night determines the time period in which the components have the status open.

Function example



Procedure 1
The closed components are opened using authorised user media. After a certain open period (of a few seconds), the components close again automatically.

Procedure 2
When the time profile starts, the components open automatically.

Procedure 3
Whilst components are in the open state, neither authorised nor unauthorised media have any effect on the state of the components. The components remain open and signal as with media with access authorisation.

Procedure 4
Once the time profile has expired, the components close again automatically.

Function example

Access authorisation will only be granted if user media are presented with UIDs or CIDs that are stored in the components.

Function example, whitelist with time profile:

Components	Media	Access
List of the UIDs stored in the components and the relevant time profiles	**UID of the presented media for a certain time**	
	Example: Friday 5 August 2014/10:15	
578AE976 “Always”	578AE976	✓
222BE121 Monday–Friday 8:00–17:00	222BE121	✓
829FE649 Sunday 10:00–12:00	829FE649	✗
—	121CA001	✗

3.9 Advanced functions

3.9.1 Wireless components

The wireless functionality is used to connect the wireless standalone components V4 to the respective system software.

The wireless functionality is an option for standalone components V4 (MRD) such as the digital cylinder and electronic c-lever fitting. The option is configured using the system software, e.g. KEM.

Advantages

- Reduced administrative effort
- Change access authorizations in real time
- Query and save events and states directly
- Display battery status
- Transfer firmware update via radio

Restrictions are:

- The function cannot be combined with TouchGo.

3.9.1.1 Overview

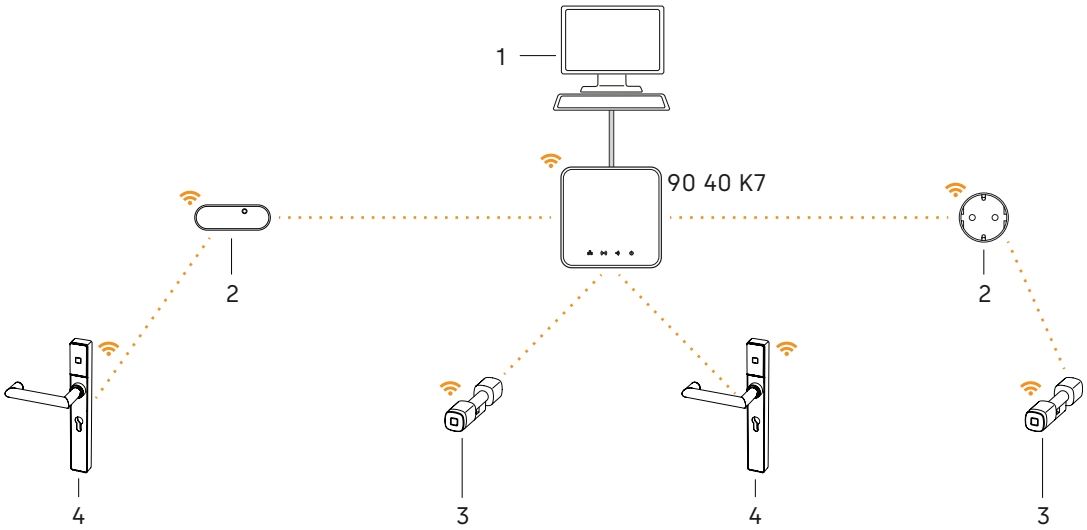
The wireless gateway is used to connect wireless components to an access control system.

The access control system is managed with a system software. With the system software, the connected devices are configured and the access rights are assigned.

Data are transferred to the system software via the Ethernet line. Data is transferred to the wireless components via radio waves.

The range of the radio connection can be extended with a wireless extender.

Topology
The graphic illustrates how the wireless gateway is integrated into a dormakaba system with wireless components and wireless extenders.



Wireless device
Wireless communication

1 Parent system
2 Wireless extender
3 Wireless component (digital cylinder)
4 Wireless component (c-lever pro)

1 System software
2 Wireless gateway
3 Wireless door component

- A maximum of 16 wireless door components can be connected to one wireless gateway.

4 Wireless extender

- A maximum of 8 wireless extenders can be connected to one wireless gateway.
- A maximum of 4 wireless extenders can be connected in series.
  (Wireless gateway → 1st wireless extender → ... → 4th wireless extender)

3.9.1.2 Taking measurements using the site survey tool

The signal quality for a wireless gateway can be measured at various locations using the site survey tool. The measurement results can be used to determine the best position for a gateway, such that all wireless components can be accessed with optimal signal quality. If the signal quality is not sufficient for secure operation, then additional gateways or extenders must be added to the system.

More information can be found in the wireless planning guidelines and in the site survey tool product description.

3.9.1.3 Taking range measurements using a wireless test medium

Alternative measurement method if the site survey tool is not available.

A detailed description of the range measurement with the gateway can be found in the separate PG Wireless manual (planning guidelines) and in the manual for the wireless gateway.

Required medium: Wireless test medium



3.9.1.4 Commissioning

Information on the procedure used to put the wireless components into operation with the help of the Programmer 1460 can be found in the manuals of the programmer, the gateway and the system software.

Principle
Wireless commissioning is started on the Gateway 90 40 K7 to which the component is supposed to connect. The programmer is used to initiate the connection sequence on the component. Once the component is successfully connected to the gateway, the component can then be configured online using the system software.

3.9.2 Component traceback

The component Traceback is a logbook file into which all the events of components are entered and stored. The function can be disabled in the system software.

Up to 2,000 events are recorded in the memory. The newest entry overwrites the oldest entry. Every entry gets a time stamp. For this purpose, the time of the component has to be correctly set. With the log, every authorized or rejected access to a door can be tracked.

For example, the following events and statuses are stored:

- Access with authorization
- Access denied for reason of absence of authorization or validation
- Access denied for reason of incorrect time window
- Setting the time
- Programming
- System test etc.

3.9.3 S-module

With the S-module, the behaviour of the component (authorisation) is overridden using an external, voltage-free contact. The S-module is activated using a switch, time switch or the building management system (e.g. alarm system). Power can be supplied to a component with an S-module using an external power supply. Batteries are no longer needed in this case.

The S-module is possible for the following components:

c-lever pro	Configurable/can be upgraded
MC cylinder	Can be upgraded
Remote reader	Present by default
Compact reader	Present by default

The S-module is configured with the help of the system software.

Restrictions are:

- It is not possible to combine S-module switching functions, Pass-Lock and pass mode.
- External power supply of the device is possible with the S-module.
- The function is not supported when operating under OSS-SO.

3.9.4 Escape return function for c-lever pro

The escape return function ensures unhindered re-entry to rooms that have been left without media in the event of an emergency (e.g. a fire).
This is because, if a person leaves the room without a medium, the room remains unlocked. The room is locked when a person leaves using their medium or presses the button.

Restrictions are:

- The function can only be used with c-lever pro components.
- The function cannot be used with the TimePro and Pass-Lock functions.
- It is not possible to combine the S-module switching functions and the re-entry function.
- External power supply of the device is possible with the S-module.

3.9.5 Pass mode with c-lever pro

Pass mode is an option for the electronic c-lever pro fitting. The function is switched on and off with a button. Through actuation of the button (no user media required), the door remains open. By once again actuating the button or by presenting an authorized user medium, the electronic fitting of the door is once again set back into the closed status. The current status of the door can be queried at any time by briefly actuating the button.
When the hardware is detected, preconfigured settings are loaded.
The pass mode is configured with the help of the system software.

Restrictions are:

- It is not possible to combine S-module switching functions, Pass-Lock and pass mode.
- External power supply of the device is possible with the S-module.

- The function is not supported when operating under OSS-SO.
- Operating pass mode via wireless is supported from firmware version 42.38.

3.9.6 Pass-Lock with c-lever pro

Pass-Lock is an option for the electronic c-lever pro fitting. The function is activated with the button on the fitting. When the button is pressed, the respective door remains closed to persons from the outside. By presenting an authorized medium (master or user), the c-lever pro is returned to open status. The door can always be opened from inside.
Pass-Lock is configured using the system software. To prevent unintended activation, a delay of 0.1–5 seconds can be configured. Pass-Lock only activates if the button is held for the full duration of the configured delay.

Limitations

- It is not possible to combine S-module switching functions, Pass-Lock and pass mode.
- External power supply of the device is possible with the S-module.
- The function is not supported when operating under OSS-SO.
- Operating Pass-Lock via wireless is supported from firmware version 42.38.
- The activation delay is configurable in the system software. The default behaviour (no delay) applies if a delay is not explicitly configured. This option is available from version 42.48 onwards.

3.9.7 Intervention media



These features is available as of firmware version 42.48 and higher.

The evolo components support a two-level authorization (2LA) model. In addition to the standard group of authorized users, a second, separately defined group of media can be assigned elevated permissions for specific access scenarios. This intervention group operates independently of the standard authorization and can be granted access in situations where normal user media are restricted or blocked, for example when Pass-Lock is active or when an intrusion detection system (IDS) is armed. The following use cases are supported:

Intervention media for Pass-lock
When Pass-Lock is active, a door is normally only returned to open status by presenting a master medium or any authorized user medium. A dedicated group of intervention media can be configured for this purpose. Only members of this group are permitted to deactivate Pass-Lock, as a difference when compared to all other authorized users. This approach is useful in situations where it is desirable to limit who can end a lockdown, such as designated security or facility personnel.

Intervention media for IDS
When an intrusion detection system (IDS) is armed, all media are normally rejected until the IDS is disarmed. A special group of intervention media can be defined to retain access even while the IDS is armed. This allows designated personnel, for example emergency services, to access the premises regardless of the alarm state.

Limitations

- Intervention media for IDS is supported only in wireless mode and requires Wireless Gateway 90 40-K7 firmware version 5.1 and higher.
- IDS arming is a MATRIX function. See the MATRIX host system documentation for configuration details.
- Intervention media are configured using the system software. Refer to the system software manual for configuration details.

3.9.8 Deactivating manual programming

The manual programming of components with media is deactivated when using the system software and the programmer 1460.

3.10 TouchGo

The electronic master key system TouchGo is an access authorization system that can be used as a standalone system or as a convenient extension of the dormakaba evolo subsystem. RCID technology forms the basis of this convenience. See section Security aspects [▶ 3.10.2].

The TouchGo system is available in two different variants. They define the scope of functions of the components. Only components of the TouchGo E310 variant are used in combination with an evolo subsystem.

A TouchGo system makes it possible to unlock doors without having to have a key or a user medium in your hand. Whether a person is carrying an authorized user medium is only recognized upon touching the component. To that end, it is enough if the user medium is carried at a distance of approx. 5–10 cm from the body, such as in a trouser pocket, jacket pocket or in a handbag for example.

Restrictions:

- TouchGo cannot be used with the wireless function.

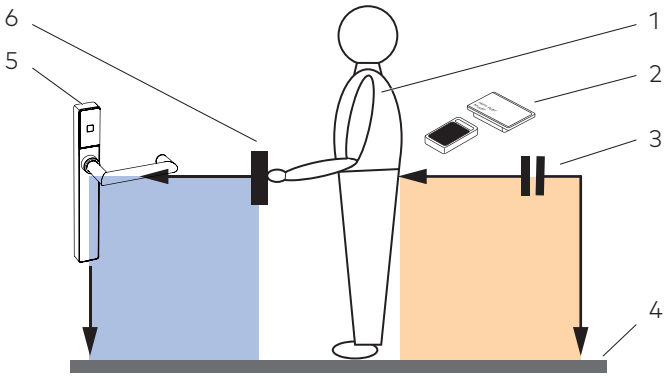
Related documents

- Planning guideline for dormakaba c-lever pro TouchGo with S-module
- User manual for dormakaba c-lever pro TouchGo

3.10.1 RCID principle of operation

RCID: Resistive Capacitive Identification

Upon contact with the component (6 to 5), an RCID medium (2) carried close to body is identified and the authorisation is evaluated.



1 Person
2 RCID media
3 Capacitive signal transfer (orange)
4 Common ground (floor)
5 TouchGo component
6 Resistive signal transfer via the lever handle (blue)

3.10.2 Security aspects

RCID technology differs from conventional solutions in that information is transferred via the electrostatic field of the body [▶ 3.10.1] without compromising comfort and security. At the same time, the flexible and secure functions of electronic master key systems are maintained. See sections Security with CardLink authorisations LEGIC [▶ 5.2] and Security with the whitelist authorisation LEGIC [▶ 5.3].

TouchGo ensures the security of the entire system at all times, because a lost user medium can be deleted easily and quickly. This prevents security gaps and eliminates the need for costly replacements of entire master key systems.

3.10.3 TouchGo E110

The TouchGo E110 can be used, with the relevant media, for a maximum of 100 users. It has the TouchGo Office mode function. The TouchGo E110 manages entirely without programming devices and system software.

The TouchGo E110 is standalone and cannot be used in an evolo subsystem.

Programming of the TouchGo E110 is described in the user manual for the c-lever pro TouchGo.

3.10.4 TouchGo E310

The TouchGo E310 components can be easily integrated in the selected system software without losing out on security. The TouchGo E310 is a convenient option that has no effect on a security configuration.

The evolo subsystem makes use of the tried-and-tested RFID technology for unique identification and management. To that end, when reading, the RFID data in the component are "married" (paired) with the data of the TouchGo technology. This means that the assigned access authorization is transferred to TouchGo and the component recognizes it through contact.

Future modifications in the authorization, transferred through the Programmer (whitelist authorization) or the RFID technology (CardLink authorization) are automatically adopted in TouchGo as well. Upon the loss or failure of the combination medium or exclusively of the pairing partner, the authorization can be immediately deleted. In other cases, the individual components can continue to be used, because a new pairing can be created at any time directly on the components.

TouchGo cannot be used with the wireless function.

3.10.4.1 Whitelist authorisation with TouchGo

In the case of master key systems with whitelist authorization, the additional comfort of TouchGo can be used for the TouchGo components. Like the RFID medium, the TouchGo RFID/RCID combination medium is simply programmed in the component with RFID programming media or placed on the desktop reader and the data of the RFID technology are registered in the system software. The access authorization of the RFID technology is distributed to the components with the Programmer. The combination medium is presented to the standalone component and when the RFID data are read, "married" (paired) with the TouchGo technology. The same access authorization is transferred to TouchGo and the component recognizes the authorization via contact.

Future modifications in the authorization are also automatically adopted in TouchGo.

3.10.4.2 CardLink authorisation with TouchGo

In the case of master key systems with CardLink authorizations too, the additional convenience of TouchGo can be used for the TouchGo components. The authorization assignment takes place in the system software and is transferred to the standalone components via the RFID technology.

Simultaneously with the transfer, TouchGo is "married" (paired). This means that the assigned access authorization is transferred to TouchGo and the component recognizes it through contact.

Future modifications to the authorization and the renewal of the validation will be transferred via the RFID technology to the standalone components, and the pairing will be examined simultaneously.

3.11 Free locker selection with cabinet lock 21 10 and 21 20

This option is only available with the cabinet lock models 21 10 and 21 20.

In the access mode CardLink or whitelist, the authorization for a locker is assigned to the user as with a normal component. In the access mode 'Free locker selection with CardLink' or 'Free locker selection with whitelist', users themselves can occupy a free locker for which they have authorization. An access mode must be configured. The number of lockers that can be occupied for the individual user is determined with the help of the locker lock wizard on the user medium. One to four lockers can be occupied. An occupied locker can only be opened with the corresponding user medium or with a service medium. The user selection is then deleted, and the locker is free again.

You can delete cabinet lock occupancies using the management tools of your host system, for example the Cabinet lock wizard in dormakaba evolo Manager (KEM).

3.12 Letterbox/lift

A user can only open those letterboxes or, in a lift, go to those floors for which they have authorization with their user medium.

The letterbox/lift can only be configured via the system software.
Mobile Access is possible with firmware version 42.38 or higher.
Wireless is not possible.

A unit consists of a remote reader 91 15 and up to six modules 90 30 with eight connected outputs each. The number of modules depends on the number of required outputs. A maximum of 49 outputs can be configured in this manner.

Ratio of outputs to needed components:

Number of outputs	Number of components
One	91 15 (remote reader with one relay output)
Up to nine	91 15 + 1 x 90 30 (extension module with eight relay outputs)
Up to 17	91 15 + 2 x 90 30
Up to 25	91 15 + 3 x 90 30
Up to 33	91 15 + 4 x 90 30
Up to 41	91 15 + 5 x 90 30
Up to 49	91 15 + 6 x 90 30

4 System variants

The evolo subsystem can be deployed in various system variants and remains expandable in all variants.

The selected examples can be implemented with LEGIC and MIFARE media, even if the pictures mainly display LEGIC. The difference is in the security cards used. For LEGIC, C1 and C2 security cards are used, and for MIFARE, only security card C.

4.1 Whitelist programming

4.1.1 Whitelist authorisation without tool chain

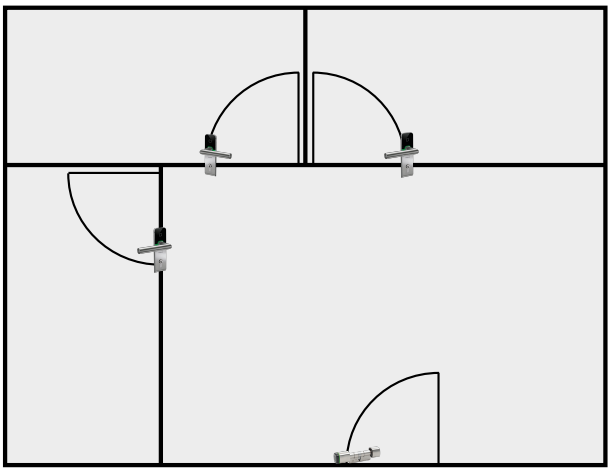
With small master key systems, the user media are directly programmed in the components with a master. System software and programmers are not required for this method. Wireless or Mobile Access are also not possible.

Programming is described in the Programming with Media section.

Master A, Master B and user media



Site example:

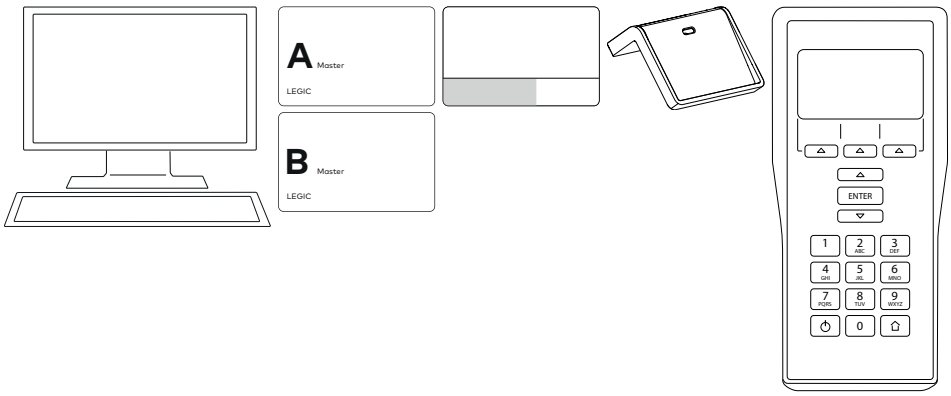


4.1.2 Whitelist authorisation with tool chain

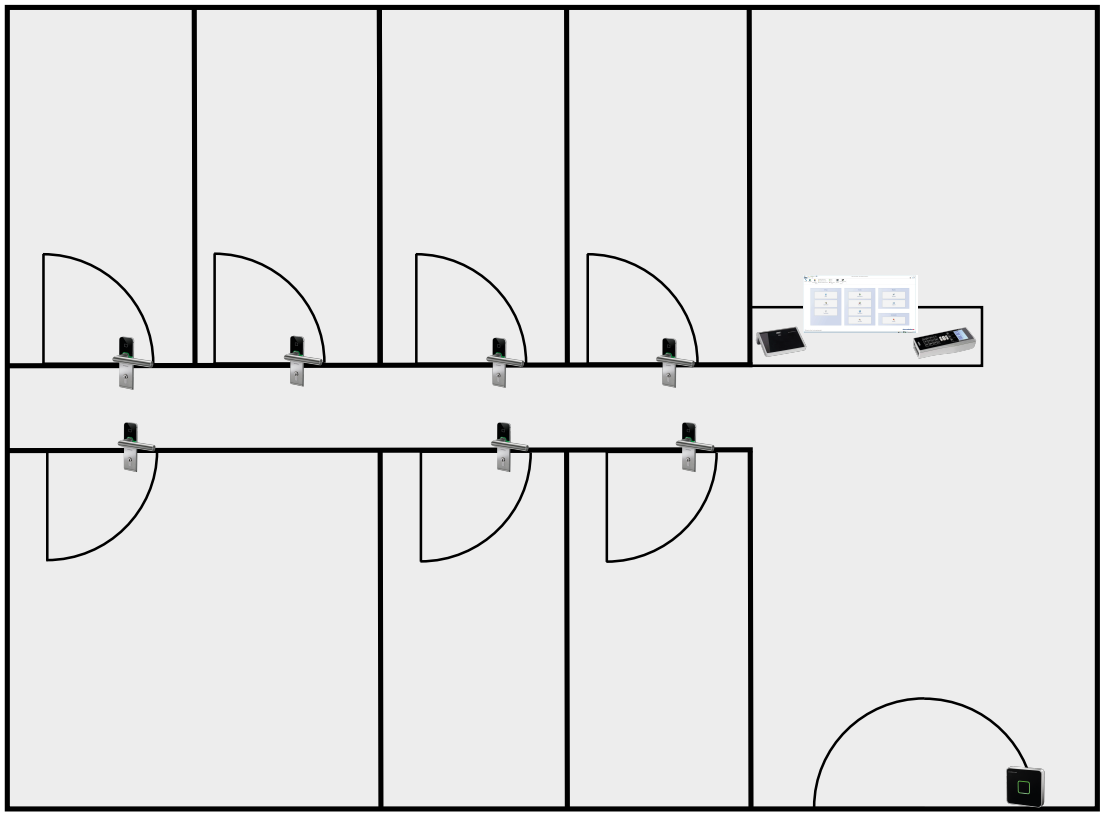
In the case of larger master key systems with time management, the user media are managed with the system software. The authorization data are transferred with the Programmer from the software into the components or updated via wireless. In the example without wireless.

Programming is described in the Programming with system software and programmer [▶ 7.5.2] section.

Tool chain: System software with master, user media, desktop reader and programmer



Site example:



4.2 CardLink programming

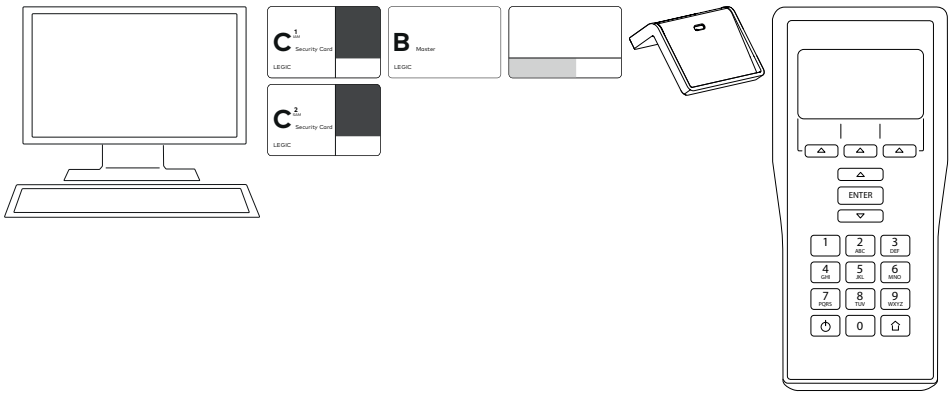
CardLink is programmed using the system software.

Programming is described in the Programming with system software section.

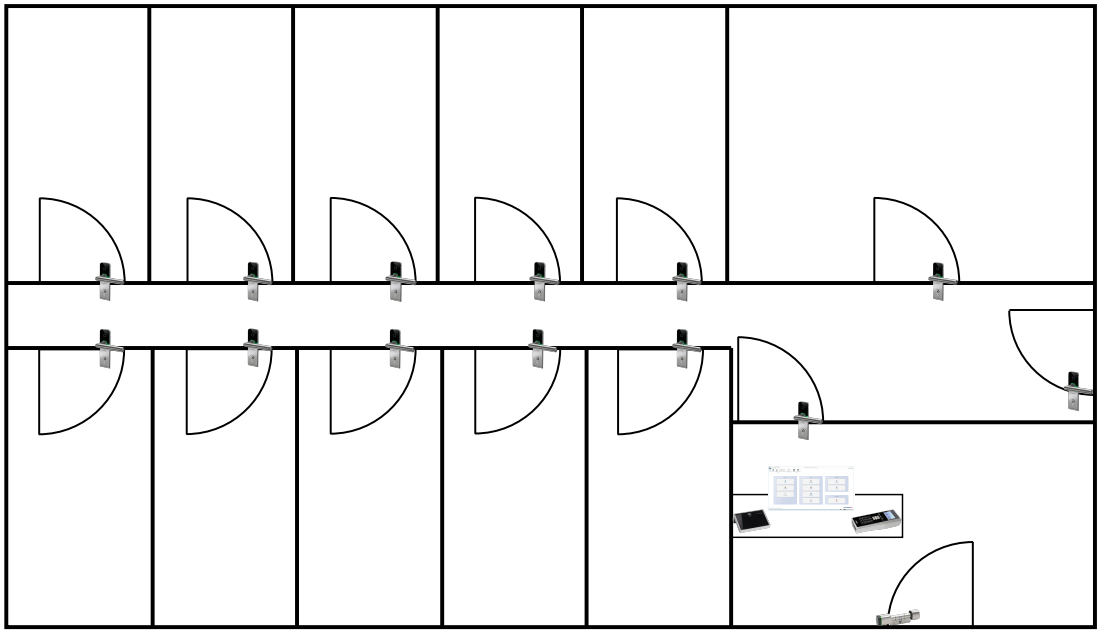
4.2.1 CardLink authorisation via desktop reader

In the case of CardLink master key systems, the user media are organized with the system software. The authorizations are written in the user media with the desktop reader. The components require only an initialization for CardLink. New authorizations are transferred by the system software into the user media with the desktop reader. In this case, validation is carried out by the individual standalone components that have been configured for this purpose. The wireless function is also supported.

Tool chain: System software with security card, master, user media, desktop reader and programmer



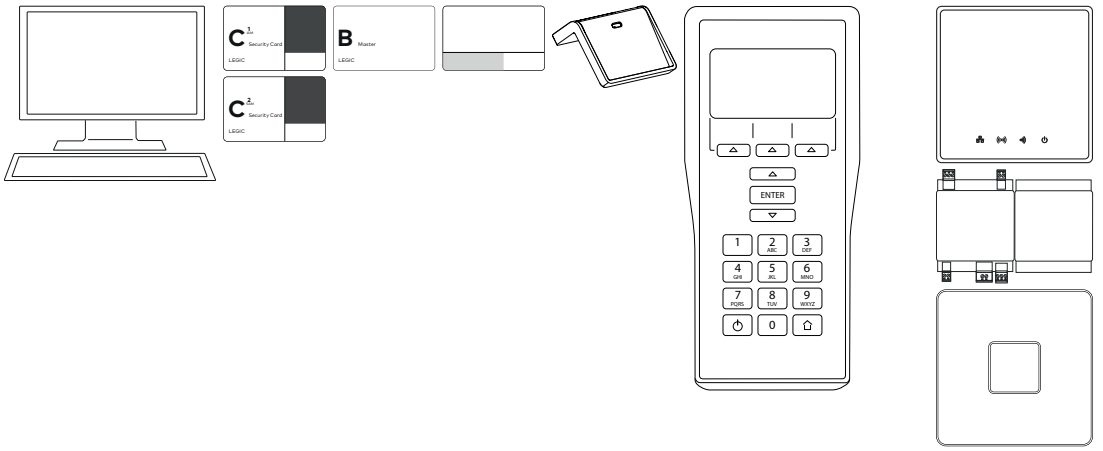
Site example:

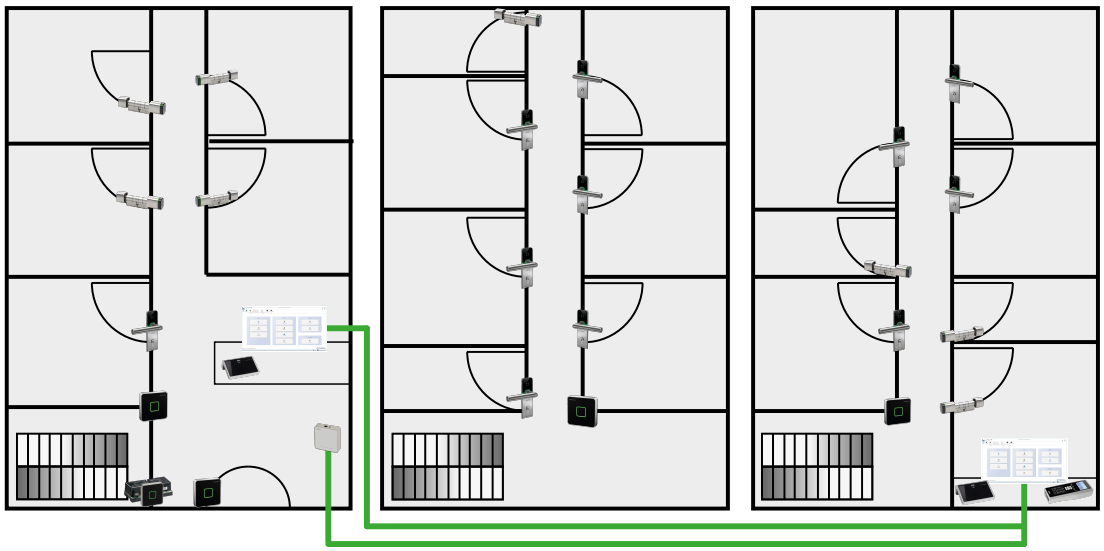


4.2.2 CardLink authorisation via update reader

For assigning new access authorizations in the user media, a CardLink update reader is used instead of the terminal. The reader is connected to the system software via a wireless gateway*. New access authorizations can thus be granted or withdrawn for the users independently of the time. In this case, the update reader takes over the validations.

Tool chain: System software with security card, master, user media, desktop reader, programmer, gateway and update reader 91 15 with extension module 90 43.





Transfer CardLink authorisations to update reader without wireless gateway

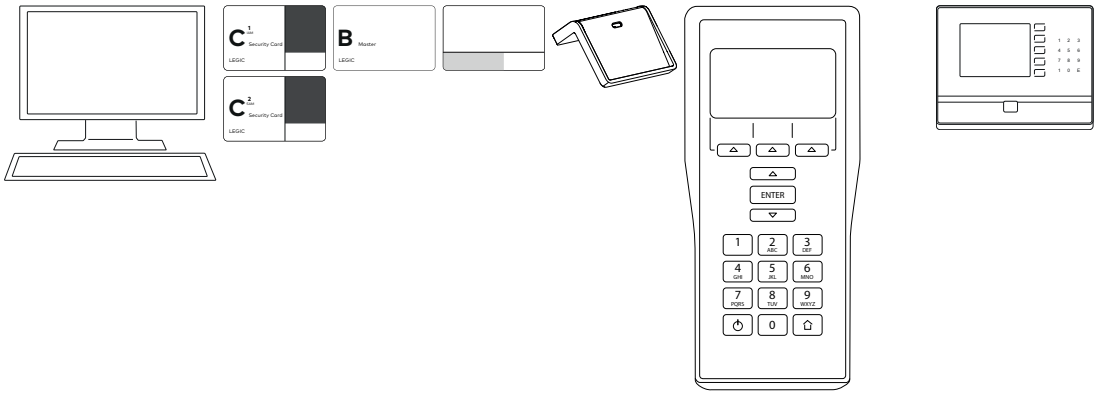
The CardLink authorisations can be transferred to the update reader with the Programmer 1460.

This does eliminate the convenience of issuing access authorisations online and at any time.

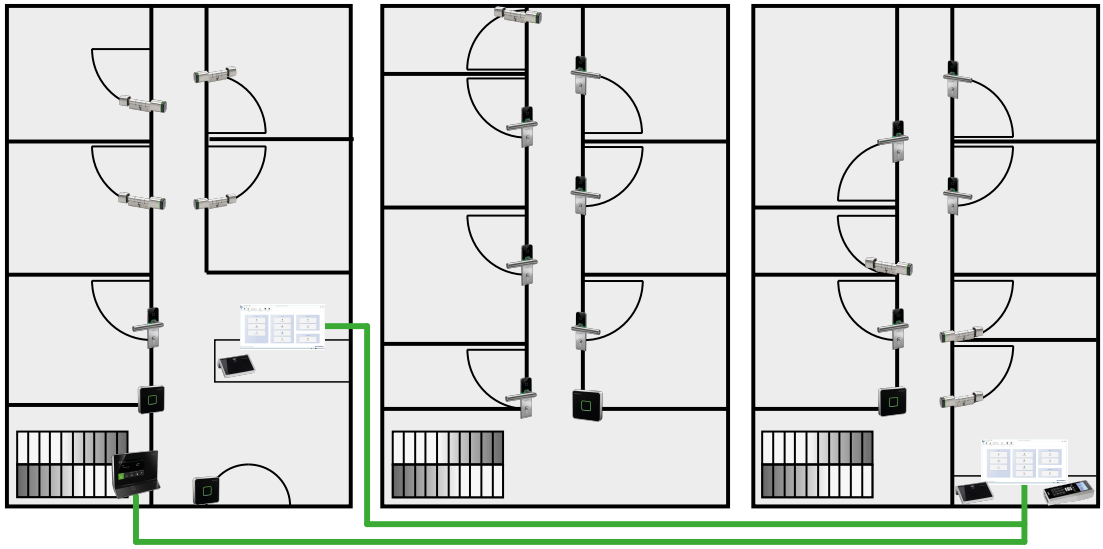
4.2.3 CardLink authorisation via terminal

This type of CardLink authorization is particularly suitable for master key systems with recurring changes in user authorizations. The terminal connected to the system software is used to assign new access authorizations to the user media. New access authorizations can thus be granted or withdrawn for users independent of time. In this case, validation is carried out by the terminal.

Tool chain: System software with security card, master, user media, desktop reader, programmer and terminal



Site example:



4.3 Firmware variant overview

Function/firmware	E300[A]	E305[B]	E310[C]	E320[D]	E321[E]	E340[F]	E360[G]	E361[H]
Master A	One	One	One	One	One	One	One	One
Master B	Up to 200	Up to 200	Up to 200	Up to 200	Up to 200	Up to 200	Up to 200	Up to 200
Whitelist authorizations								
Whitelist (UID/Card ID) entries - offline mode	4,000	1,000	1,000[5]	4,000	4,000 (offline mode)	4,000	4,000 (offline mode)	4,000 (offline mode) Up to 30,000 (online use with 90 40K7 gateway)
Whitelist (UID/Card ID) entries - online mode using Wireless Gateway 90 40K7				Up to 30,000	Up to 30,000		Up to 30,000	Up to 30,000
Time-dependent authorizations	✓	✓	✓	✓	✓	✓	✓	✓
Deactivate manual programming	✓	✓	✓	✓	✓	✓	✓	✓
CardLink authorizations								
Validation	✓	—	✓	✓	✓	✓	✓	✓
Individual right, door[4]	Up to 60	—	Up to 60	Up to 60	Up to 60	Up to 60	Up to 60	Up to 60
Individual right, door group[4]	Up to 39	—	Up to 39	Up to 39	Up to 39	Up to 39	Up to 39	Up to 39
Reservation individual right door[4]	Up to 18	—	Up to 18	Up to 18	Up to 18	Up to 18	Up to 18	Up to 18
Reservation individual right door group[4]	Up to 11	—	Up to 11	Up to 11	Up to 11	Up to 11	Up to 11	Up to 11
Door group right	512	—	512	512	512	512	512	512
Blacklist entries	400	—	400	400	400	400	400	400
Service media	✓	—	✓	✓	✓	✓	✓	✓
Media traceback[3]	60	—	60	60	60	60	60	60
TouchGo media	—	—	1,000	—	—	—	—	—
Expanded functions								
Wireless	—	—	—	✓	✓	—	✓	✓
Components traceback memory	2,000	2,000	2,000	2,000	2,000	2,000	2,000	2,000
Pass mode[1]	Option	—	Option	Option	Option	Option	Option	Option

Function/firmware	E300[A]	E305[B]	E310[C]	E320[D]	E321[E]	E340[F]	E360[G]	E361[H]
Time profiles	15 and "Always"	15 and "Always"	15 and "Always"	15 and "Always"	15 and "Always"	15 and "Always"	15 and "Always"	15 and "Always"
Time window for every time profile	12	12	12	12	12	12	12	12
Holiday periods	20	20	20	20	20	20	20	20
Special days A+B	32+32	32+32	32+32	32+32	32+32	32+32	32+32	32+32
TimePro functions	✓	✓	✓	✓	✓	✓	✓	✓
S module[2]	Option	—	Option	Option	Option	Option	Option	Option
Master T and service medium	✓	✓	✓	✓	✓	✓	✓	✓
Mobile Access								
NFC/HCE	✓	—	—	✓	✓	✓	✓	✓
Bluetooth	—	—	—	—	—	✓	✓	✓

Legend:

1 Only for c-lever pro.

2 Default for reader, optional for c-lever pro.

3 Only with MIFARE DESFire and LEGIC advant media.
Depending on the segment/file size
Default value as per media specification. Can be larger or smaller.

4 Depending on the authorization types used.

5 RCID and RFID.

A E300 – evolo V4

B E305 – Letterbox/lift
E345 – Letterbox/lift with Mobile Access

C E310 – TouchGo

D E320 – Wireless

E E321 – Wireless with door monitoring
Additional components, such as door frame contacts and lock sensors (latch, bolt), are required.

F E340 – Mobile Access

G E360 – Wireless and Mobile Access

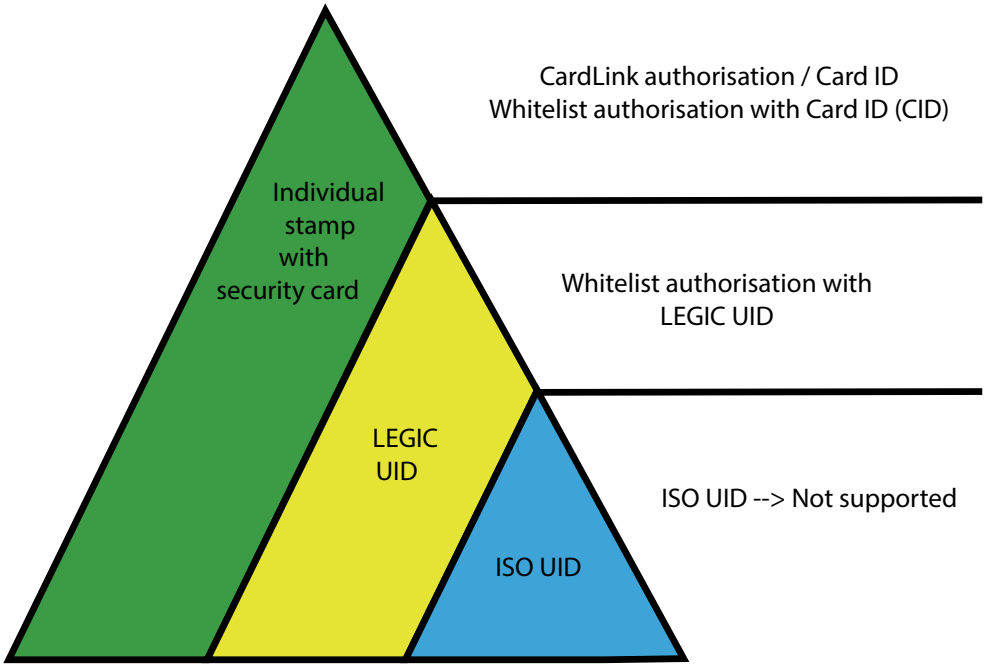
H E361 – Wireless with door monitoring and Mobile Access
Additional components, such as door frame contacts and lock sensors (latch, bolt), are required.

5 Security functions

This chapter describes the possible security functions for LEGIC and MIFARE in locking systems, which can be selected according to security requirements.

5.1 LEGIC security levels

The following security levels are available for the various types of authorisation.



Individual stamp
An individual stamp is defined for every locking system. This stamp serves to identify the site-specific LEGIC media. The stamp is defined by the security card C1 or C2 in the respective locking system.

LEGIC UID
The LEGIC UID is used for normal locking systems with Whitelist. With LEGIC UID, the unique number (UID) is also verified via a LEGIC function on the media.

Note: The KEM system software solely uses the LEGIC UID.

5.2 Security with CardLink authorisations LEGIC

Individual stamp
When a CardLink authorization is used, an individual stamp is required with LEGIC.

Every electronic component as well as the desktop reader have LEGIC hardware that work with this stamp. In order that the system-specific stamp can be integrated in the master key system, the security card C1 and/or C2 is required. With this security card, the stamp is transferred to the respective component. A new security card is needed for every master key system. If a stamp is used, the system software KEM, the desktop reader and the respective components should be initialized with it. Then, the security card must be stowed in a secure location (for example, the safe).

5.3 Security with the whitelist authorisation LEGIC

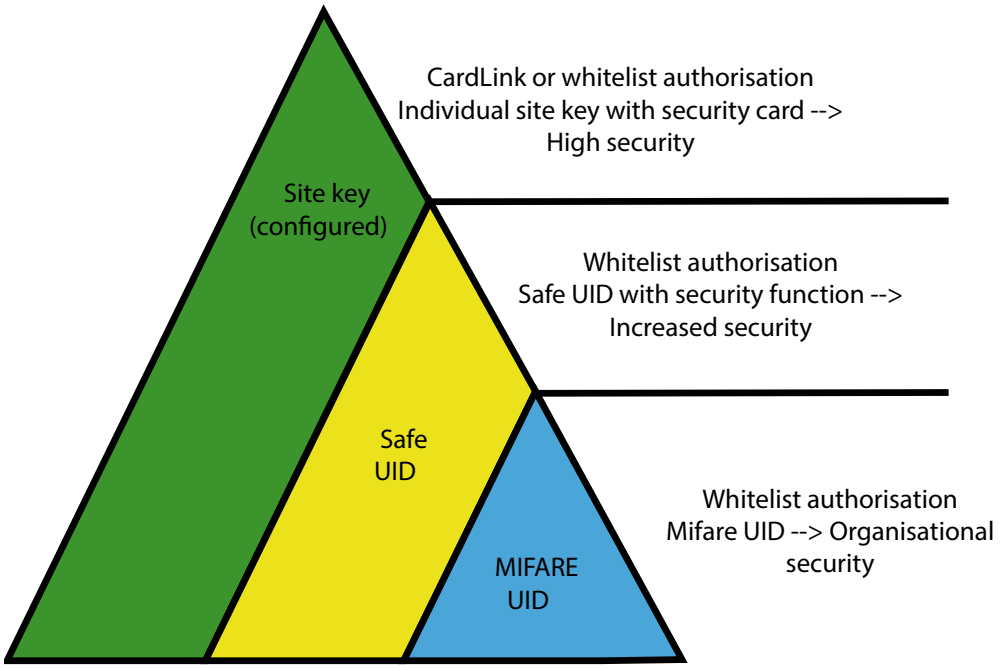
Card ID (CID)
Instead of the UID, the system assigns an individual CID to the media.

This CID is written into the media memory with an individual LEGIC stamp. This stamp is defined via the security card C1. A separate security card is required for every site so as to guarantee security. If the individual LEGIC stamp is used, the system software KEM and the desktop reader should be initialized with it. Then, the security card must be stowed in a secure location (for example, the safe).

LEGIC UID
In the case of LEGIC UID, the LEGIC function is used for securing the UID (unique number) of the user media. The security of a UID is significantly improved, since the LEGIC function verifies the UID.

5.4 MIFARE security levels

The following security levels are available for the various types of authorisation.



Site key
A site key may be suitable for insertion in locking systems with high security demands.

The site key is a specific key that is assigned on an individual basis to each individual locking system. This key is produced automatically by a security chip. This additional security chip is integrated in every component and, once it has been initialised, it manages the individual encoding and decoding of all data that the system writes to the user media.

Safe UID
This security level is used for average locking systems.

With Safe UID, the unique number (UID) undergoes additional encryption and is then saved to the media memory. The UID is only recognised as valid if the data in the user media matches.

MIFARE UID
This security level is suitable primarily for organisational applications.

MIFARE media comply with ISO standard 14443A. This standard specifies that it must be possible to read the unique number (UID) with no additional key. With this level of security, only the transponder UID is used for identification.

5.5 Security with CardLink authorisations MIFARE

Site keys
With the use of a CardLink authorization or a Master T, a site key becomes necessary.

Every electronic component as well as the desktop reader have the special security hardware that work with this site key. In order that the specific key can be integrated in the master key system, the security card C of the relevant site is required. With this security card, the site key is transferred to the respective master key system. An individual security card is needed for every master key system.

If a site key is used, the system software, the desktop reader and the respective programming media should be initialized with it. Then, the security card must be stowed in a secure location (for example, the safe).

5.6 Security with the whitelist authorisation MIFARE

Card ID (CID)
Instead of the UID, the system assigns an individual CID to the media. This CID is encrypted with an individual site key and written to the media memory. This site key is defined by a security card C.

The security card C can be procured from the sales division. With this security card, the electronic components are initialized with the individual key of the site. An individual security card is needed for every site.

If a site key is used, the system software, the desktop reader and the respective programming media should be initialized with it. Then, the security card must be stowed in a secure location (for example, the safe).

Safe UID
The security level Safe UID is suitable for applications with increased security demands.

The requirement for the use of the Safe UID is the Kaba application KCA in the user media. With the Safe UID, the UID (unique number) of the media is additionally checked by a special application in the media memories. The security of a UID is significantly improved as a result, since the content of the application is not freely accessible and encrypted.

MIFARE UID (as per ISO 14443A)
An authorization can be programmed with the UID (unique number) in the whitelist.

If the UID conforms to the ISO 14443A standard, it can be entered in the whitelist. According to the ISO standard, this UID is freely readable and not secured further. The use of this security level is only recommended for organizational applications with a low security requirement.

5.7 Master T

Master T is a special form of the master media for standalone components. Master Ts used in a master key system are only valid for a certain time and have limited functions. This facilitates a high level of flexibility in the management of master key systems, because a Master T can be issued to service personnel, as opposed to the security-relevant Master A or B.



A Master T can only be used if the components have been previously configured with a Master B and the Programmer 1460.

Master T for LEGIC:
Master T media can be defined for LEGIC using the system software. A Master T is extrapolated from the security card and can only be used as a Master T.

Master T for MIFARE:
Master T media can be defined for MIFARE using the system software. A Master T can be extrapolated from security card C.

The Master T media for LEGIC and MIFARE have the following properties:

- Application in both authorization types: CardLink and whitelist.
- Updating the components (the components must be configured).
- Setting the clock of the components.
- Reading traceback.
- A period limited period of validity.

6 Components

The evolo components offer a large number of various functions that are summarized in the following overview. For security-relevant ranges, mechanically strengthened protection components are available. Detailed information can be found in the separate user manuals and the product catalogue.

6.1 Memory sizes

The following storage sizes are available for the rewritable memories of the user media:

	MIFARE		LEGIC
Authorizations	**classic**	**DESFire**	**advant**
	In bytes	In bytes	In bytes
Memory size of the user media	1 k	8 k	4 k
CTC user media	—		3 k
Memory size of the default applications	288	744	848
Kaba Common Application (KCA) Safe UID	48	32	—
CardLink (192 bytes of useful data)	216	192	216
Maximum number of authorizations on a user medium:			
Maximum of 512 door groups configured:	– up to 39 individual rights – up to 11 reservations		
Without door groups:	– up to 60 individual rights – up to 18 reservations		
Status entries:			
Status components (32 bytes of useful data)	48	32	56
Identification (32 bytes of useful data)	48	32	64
Traceback (60 entries)	—	488	512

6.2 Technical data

User media
Cards

Name	**Values**
Colours (Print layout)	• dormakaba (red or blue) • your custom design
Ambient conditions	
Degree of protection	IP66 Can sustain being wet, but not submerged in water. For example, usage as a swimming pool key is not recommended.
Temperature	-25 ... +70 °C
Humidity	0 ... 95% RH, non-condensing
Media memory capacity	
K-BE-MID	8 kB (MIFARE DESFire EV3)

K-BE-MIC	1 kB (MIFARE classic)
K-BE-ADT	4 kB/3,5 kB (LEGIC advant/MIFARE DESFire EV3)
K-BE-CTC	1kB/3kB (LEGIC prime/advant)

The cards are protected against hacking or cloning

Key fob

Name	**Values**
Colours	Blue, black, red, white
Ambient conditions	
Degree of protection	IP65
Temperature	-20 ... +55 °C
Humidity	0 ... 95% RH, non-condensing
Media memory capacity	
A-BE-MID	8 kB (MIFARE DESFire EV3)
A-BE-ADT	4 kB/3,5 kB (LEGIC advant/MIFARE DESFire EV3)
A-BE-CTC	1kB/3kB (LEGIC prime/advant)

Key with clip

Name	**Values**
Clip	
Colours	
Clip colour inserts	Black, silver, violet, yellow, green, red, blue
Ambient conditions	
Degree of protection	IP67 Can sustain being temporarily submersed in water.
Temperature	-20 ... +70 °C
Humidity	0 ... 95% RH, non-condensing
Media memory capacity	
S-BE-MID	8 kB (MIFARE DESFire EV3)
S-BE-MIC	1 kB (MIFARE classic EV1)
S-BE-ADT	4 kB/3,5 kB (LEGIC advant/MIFARE DESFire EV3)
S-BE-CTC	1kB/3kB (LEGIC prime/advant)
Key	
Mechanical Locking Systems	
dormakaba eco	
dormakaba expert	
dormakaba gemini	
dormakaba matrix	
dormakaba penta	
dormakaba quattro	
dormakaba pextra	
dormakaba AP2000	
Kaba star	

Kaba star cross
Kaba 20

TouchGo user media
Key fob

Name	**Values**
Colours	
User media	Black, white
Dimensions	
W x H x D	36 x 60 x 12 mm
Power supply	
Battery	3V CR2450 lithium
Ambient conditions	
Degree of protection	IP 53
Temperature	-25 ... +65 °C
Humidity	0 ... 95% RH, non-condensing
Media memory capacity	
A-BE-TGO	
A-BE-TGO-MID	8 kB (MIFARE DESFire EV3)
A-BE-TGO-MID-ADT	4 kB/3,5 kB (LEGIC advant/MIFARE DESFire EV3)
A-BE-TGO-MID-CTC	1kB/3kB (LEGIC prime/advant)

Wristband

Name	**Values**
Colours	Grey
Dimensions	
W x H x D	56 x 53 x 17 mm
Power supply	
Battery	3V CR2450 lithium
Ambient conditions	
Degree of protection	IP67 (waterproof)
Temperature	-25 ... +65 °C
Humidity	0 ... 95% RH, non-condensing
Media memory capacity	
B-BE-TGO	8 kB (MIFARE DESFire EV3)
B-BE-TGO-MID	1 kB (LEGIC prime)
B-BE-TGO-ADT	4 kB/3,5 kB (LEGIC advant/MIFARE DESFire EV3)
B-BE-TGO-CTC	1kB/3kB (LEGIC prime/advant)

Card holder

Name	**Values**
Colours	
Card holder	Black, silver black
Dimensions	
W x H x D	90 x 58 x 14 mm

Power supply	
Battery	3V CR2430 lithium
Ambient conditions	
Degree of protection	IP 53
Temperature	-25 ... +65 °C
Humidity	0 ... 95% RH, non-condensing
Media memory capacity	
H-BE-TGO	depending on inserted medium.

6.3 Master media

With two different types of master media, Master A and Master B, the components can be set in programming mode (). These media are used exclusively for granting the authorization and do not have any access authorization themselves.

Master media	MIFARE	LEGIC	Functions
Master A 	✓	✓	– Master of a site with Master A/B structure – Components are put into the programming mode with Master B – Programming components with Master B
Master B 	✓	✓	– Master of a site – Components are put into the programming mode – Programming components with user media
Master T 	✓	✓	– Master T for updating components – Only valid for a limited time – Restricted functions
RCID Master B 			RCID only TouchGo E110 – Master of a site – Components are put into the programming mode – Programming components with user media

6.4 Security cards

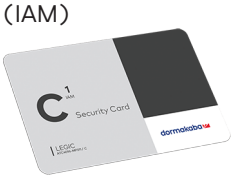
The security cards are used in a LEGIC or in a MIFARE environment. Depending on the technology used, the functions of the security cards differ.

For LEGIC, there are miscellaneous security cards:

- Security card C1 for site-specific segmentation of media
- Security card C2 for initializing the site with desktop readers and validation components in CardLink

For MIFARE, there is security card C:

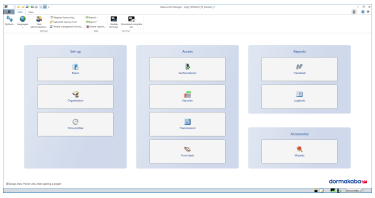
In order that the site-specific key of a MIFARE environment can be integrated in the master key system, security card C is required. It defines the site key as well as the memory organization of the user media.

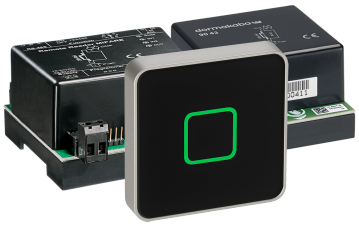
Security cards	MIFARE	LEGIC	Functions
Security card C 	✓	—	– Definition of site key – Configuring the media – Initializing the system – Writing applications to empty cards
Security card C1 (IAM) 	—	✓	– Definition of the stamp – Initializing the system – Configuring the media – Creating segments
Security card C2 (SAM) 	—	✓	– Definition of the stamp – Initializing the system – Write authorization for desktop readers and validation component – Writing on segments

Write authorization with security card C2
With security card C2 components that are to write data to the segments on the user media will get a write authorization. They are, for example, desktop readers or validation components. For a description of the application, see chapter Messages when using the security card C2 [▸ 8.5].

6.5 Tool chain

A tool chain comprises of the programming tools used in the subsystem. The tools have various functions for configuring, managing, reading from, and writing to components and media.

Tool	Functions
Programmer 1460 	• Configuring component properties. • Programming of components. • Reading the traceback of components. • Firmware updates on components. • Putting wireless components into operation.
System software: e.g. dormakaba evolo Manager (KEM). 	• Management of authorizations. • Management of media and persons. • Management of master key systems. • Evaluation of traceback data.
Desktop reader 91 08 	• Reading from and writing to media. • Organization of the media memory.

Tool	Functions
Wireless Gateway 90 40-K7 	• Configuring component properties. • Programming of components. • Reading the traceback of components. • Firmware updates on components.
Wireless Extender 90 41 	• Extending the range of the wireless gateway. • For wireless components.
Wireless extension on the remote reader 	91 15 + 90 43 • Wireless link for remote readers. • CardLink update via wireless.
Mobile Access 	Mobile Access • Management/access via smartphone with Bluetooth or NFC.

7 Program/configure a component

The media technology must be defined before programming. See section Define media technology [▶ 7.1].

Access permissions and other permissions are assigned through subsequent programming/ configuration of the components.

- Wireless components require wireless commissioning prior to initial use.
  See wireless documentation

7.1 Define media technology

Upon first use, multi RFID (MRD) components are defined using a master LEGIC or MIFARE for the technology for which the components are to be operated. After that, the components act as defined for the authorisation types LEGIC (LEA) or MIFARE (MID).

Procedure

- Hold the master medium up to the antenna for approx. 1 second.
  - The media technology of the master medium (Legic or MIFARE) has been transmitted to the device.

Note: After an INI reset, the technology must be redefined.

7.2 Methods for programming and configuration

Methods:

- Without host system with master and user media,
  See Section Programming with media [▶ 7.4]
- With system software and programmer,
  See Section Programming with system software and programmer [▶ 7.5.2]
- TouchGo products:
  See section Programming TouchGo products.
- Wireless applications:
  Commissioning with system software and programmer,
  after which configuration takes place via wireless gateway.
  See programmer manual, wireless gateway manual and system description.
- Mobile Access devices: After transmitting the configuration using the programmer: Initialise the device for Mobile Access,
  See section Initialising the device for Mobile Access [▶ 7.6.2]
- evolo smart:
  The app guides the user through the procedure.

7.3 Programming TouchGo products

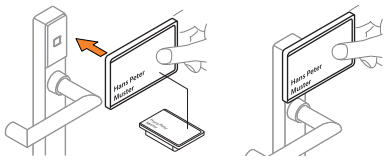
With TouchGo, the access authorization is checked when the components are touched.

Product	
c-lever pro TouchGo E110	RCID only; standalone whitelist See user manual for dormakaba c-lever pro TouchGo
c-lever pro TouchGo E310	RFID and RCID; evolo subsystem See section Programming TouchGo E310.

7.3.1 Programming TouchGo E310

With TouchGo E310, RFID media are used for the programming. For the TouchGo function to become active, pairing of RFID and RCID user media must be done after the programming.

Use master media and user media of the TouchGo E310 as follows:



Hold RFID master media and combi-media (RCID/RFID user media) if using TouchGo E310 up to the RFID registration unit (illumination unit).

7.3.1.1 Manual whitelist programming

7.3.1.1.1 Programming user media

After holding up the master B, the component receives the following temporary right:

- Grant the access authorisation to the user medium presented (enter in whitelist).

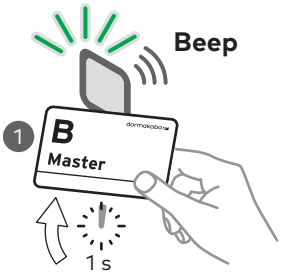
After presenting the master B again or after 20 seconds of not presenting a medium, the temporary right of the component is withdrawn.

Requirements

- A/B structure or
- B structure is available

Procedure:

1. Hold master B up to the registration unit for approx. **1 second**.

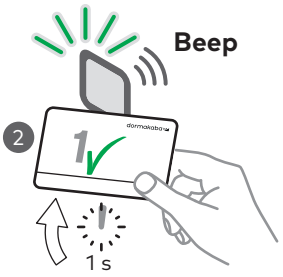


   ⇨ Green glows.
   ⇨ After a short acoustic signal,
   ⇨ Green light goes out.

If no medium is presented for 20 seconds, the process ends automatically:

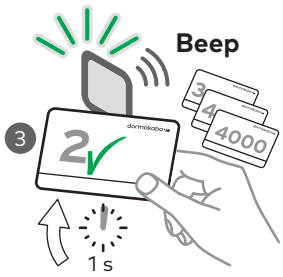
-> The modifications have been made and 1 long signal sounds.

2. Hold the user medium up to the registration unit for approx. **1 second**.

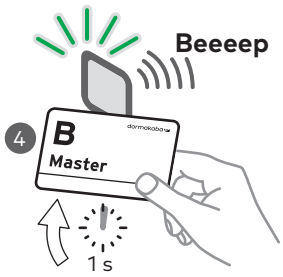


   ⇨ Green glows.
   ⇨ After a short acoustic signal,
   ⇨ Green light goes out.
   ⇨ The user medium has been entered into the whitelist.
   ⇨ The user medium has access to the component.

Programming other user media: Repeat step 2.



3. Hold master B up to the registration unit for approx. 1 second.



⇨ Green glows.

⇨ 1 long acoustic signal.

⇨ Green light goes out.

⇨ The changes have been made.

⇨ Programming is complete.

Grant access authorisations with other master B if needed.

7.3.1.1.2 Cancel individual authorisation

Cancel the access authorisation of a user medium.

After holding up the master B, the component receives the following temporary right:

- Revoke the access authorisation to the user medium presented (remove from the whitelist).

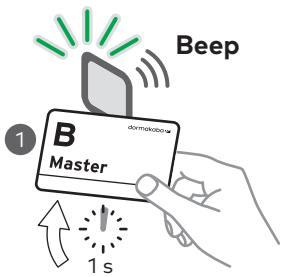
After presenting master B again, the temporary right of the component is withdrawn.

Requirements

- User medium with access authorisation.
- A/B structure or
- B structure is available

Procedure
Present other user media if needed.

1. Hold master B up to the registration unit for approx. **1 second**.



⇨ Green glows.

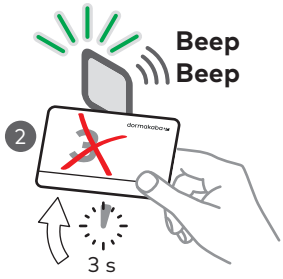
⇨ After a short acoustic signal,

⇨ Green light goes out.

If no medium is presented for 20 seconds, the process ends automatically:

-> The modifications have been made and 1 long signal sounds.

2. Hold the user medium up to the registration unit for approx. **3 seconds**.



⇨ Green glows.

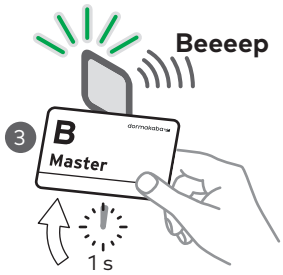
⇨ 2 short signals sound.

⇨ Green light goes out.

⇨ The user medium has been removed from the whitelist. The user medium does not have access to the component.

Present other user media if needed.

3. Hold master B up to the registration unit for approx. 1 second.



⇨ Green glows.

⇨ 1 long acoustic signal.

⇨ Green light goes out.

⇨ The changes have been made.

⇨ The process is complete.

7.3.1.1.3 Cancelling all access authorisations

After holding up the master B, the component receives the following temporary right:

- Cancel all access authorisations granted by the master B (remove from the whitelist).

Note: The master B has the right to grant access authorisations.

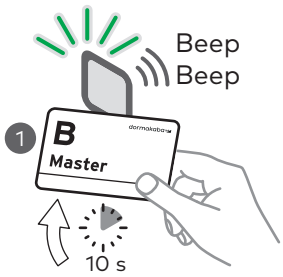
Procedure

NOTICE

Data loss

If the master B is presented for **15 seconds**, the INI reset is initiated.
The INI reset deletes all the settings and data saved in the component.

1. Hold master B up to the antenna for approx. **10 seconds**.



⇨ Green glows.

⇨ Firmware version 42 and above: 1 long and 2 short signals sound.
Pre-firmware version 42: 2 short signals sound.

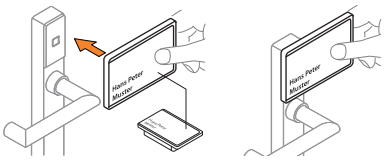
⇨ Green light goes out.

⇨ All access rights assigned by master B have been cancelled.

⇨ The process is complete.

7.3.1.2 RCID/RFID pairing

The TouchGo E310 is used in the dormakaba evolo system. The RFID technology is used for programming and identification. For the TouchGo function to become active, pairing of RFID and RCID user media is necessary.



7.3.1.2.1 Granting RCID authorisation

Whitelist authorisation

The authorisation is programmed with the RFID master medium and the combi-media (RCID/RFID user media) directly via the RFID registration unit. When reading the combi-medium, the RFID data is "paired" with the RCID data (TouchGo).

CardLink authorisation

The authorisation is set up via the system software and is used with the combi-media (RFID/RCID user media) directly via the RFID registration unit. When reading the combi-medium, the RFID data is "paired" with the RCID data (TouchGo).

Future modifications in the authorisation and the update of the validation will be transferred with the RFID technology to the components and simultaneously, the pairing will be examined.

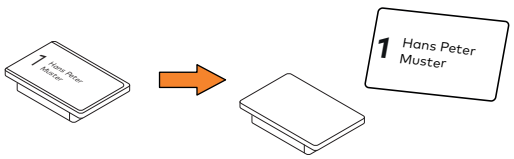
RCID media cannot be programmed twice (already existing pairing).

7.3.1.2.2 Cancelling RCID authorisation

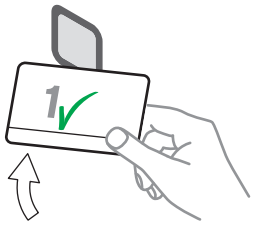
Cancel the RCID authorisation by separating the RCID/RFID pair. This is not possible in combi-media.

Procedure

1. Physically separate RFID medium and RCID medium.
   E.g. remove the card from the card holder.



2. Place the RCID medium approx. 2 m away on another table.
   ⇨ Do not carry the RCID medium on your person.
3. Hold the RFID medium up to the component.



⇨ Pairing is cancelled.

7.3.1.3 Parameterise TouchGo E310 in system software

TouchGo E310 components can also be operated in master key systems that are managed with system software. The combi-media (RCID/RFID user media) are programmed in the component with a RFID master medium, or the RFID data is registered and managed with the desktop reader. The access authorisations of the combi-medium are then transferred with the programmer (whitelist authorisation) or the RFID data of the combi-medium (CardLink authorisation) to the components.

7.3.1.4 TimePro function

7.3.1.4.1 Office mode in whitelist

1 medium with TimePro:

The operation is analogue to the operation of office mode.
The TimePro function enables a time-controlled activation.

Multiple TimePro entries:

Activation through the combi-medium or the TouchGo function (touch internal lever handle).
Deactivation through the combi-medium or the set time window.

7.3.1.4.2 Office mode in CardLink

Activation of the TimePro function or the office mode through the combi-medium or through TouchGo (touch internal lever handle).
Deactivation through the combi-medium or the set time window.

7.3.1.5 Programming office mode authorisations

The TouchGo office mode function is described in the Operation section.
This section describes the granting or cancelling of the authorisation, in order to activate or deactivate office mode.

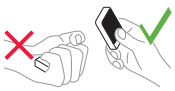
E310
The authorisations are assigned to the user with the help of the system software.

E110
Programming in TouchGo E110:

- Granting authorisation: Section [▸ 7.3.1.5.1]
- Cancelling authorisation:
  - Individual authorisation: Section [▸ 7.3.1.5.2]
  - All authorisations: Section [▸ 7.3.1.5.3]

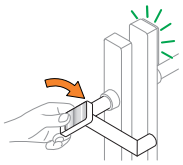
7.3.1.5.1 Granting office mode authorisation

- Do not clasp your hand around the master medium and the user medium.



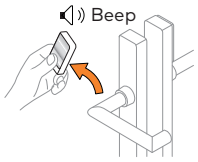
- Only pick up 1 medium. Ensure that other media are at least 2 m away.

1. Pick up the master medium.
2. Touch the internal lever handle with your index finger.



⇨ Green glows.

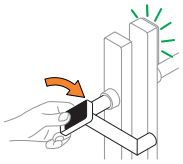
3. Remove index finger/master medium.



⇨ Green light goes out.

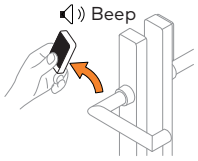
⇨ After a short acoustic signal,

4. Pick up the user medium.
5. Touch the internal lever handle with your index finger.



⇨ Green glows.

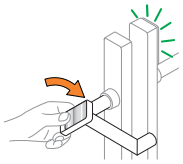
6. Remove index finger/user medium.



⇨ Green light goes out.

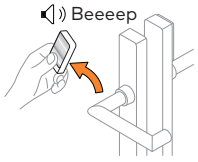
⇨ After a short acoustic signal,

7. Pick up the master medium.
8. Touch the internal lever handle with your index finger.



⇨ Green glows.

9. Remove index finger/master medium.



⇨ Green light goes out.

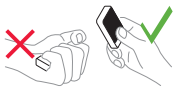
⇨ 1 long acoustic signal.

⇨ The office mode access authorisation has been granted.

7.3.1.5.2 Cancelling individual office mode authorisation

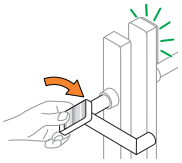
Cancel the office mode authorisation of a user medium.

- Do not clasp your hand around the master medium and the user medium.



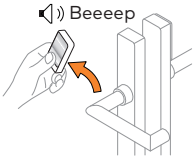
- Only pick up 1 medium. Ensure that other media are at least 2 m away.

1. Pick up the master medium.
2. Touch the internal lever handle with your index finger.



⇨ Green glows.

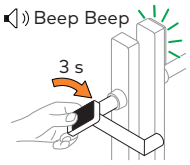
3. Remove index finger/medium.



⇨ Green light goes out.

⇨ 1 long acoustic signal.

4. Pick up the user medium.
5. Touch the internal lever handle with your index finger for 3 seconds.

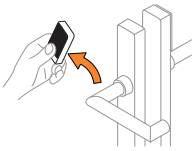


⇨ Green glows.

⇨ 2 short signals sound.

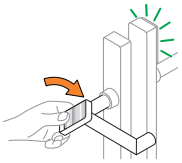
⇨ The office mode authorisation of the medium is cancelled.

6. Remove index finger/user medium.



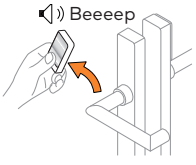
⇨ Green light goes out.

7. Pick up the master medium.
8. Touch the internal lever handle with your index finger.



⇨ Green glows.

9. Remove index finger/master medium.



⇨ Green light goes out.

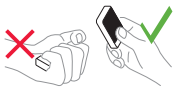
⇨ 1 long acoustic signal.

⇨ The office mode authorisation is cancelled.

7.3.1.5.3 Cancelling all office mode authorisations

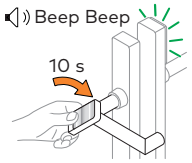
Cancel all office mode authorisations saved in the components.

- Do not clasp your hand around the master medium and the user medium.



- Only pick up 1 medium. Ensure that other media are at least 2 m away.

1. Pick up the master medium.
2. Touch the internal lever handle for 10 seconds.

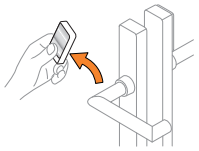


⇨ Green glows.

⇨ 2 short signals sound.

⇨ All authorisations are cancelled.

3. Remove index finger/master medium.



⇨ Green light goes out.

⇨ All office mode authorisations are cancelled.

7.3.2 Lost/defective user media

It is necessary to cancel the authorisations of lost or defective user media for the safety of the system. The authorisations of the remaining user media are then reprogrammed.

Workflow:

1. Cancel all authorisations. See [▸ 7.3.1.1.3]
   ⇨ The access authorisations will be cancelled.
   ⇨ The office mode authorisations will be cancelled.
2. Reprogram the user media.
   ⇨ Reprogram the access authorisations. See [▸ 7.3.1.1.1]
   ⇨ Reprogram the office mode authorisations. See [▸ 7.3.1.5]

7.4 Programming with media

Holding up a Master medium (approx. 1 s) activates programming mode.
Leaving programming mode:
Automatic, 20 s after the last medium was held up (timeout) or
by holding up the Master medium again (approx. 1 s).

7.4.1 Cards

7.4.1.1 Define highest Master medium

- The highest Master medium is the highest medium of a component.
- Each component must be assigned 1 highest Master medium.
- Each component can only be assigned 1 highest Master medium.
- The first Master medium that is held up to a component will be registered as the highest Master medium.

A/B structure

- In an A/B structure, the highest Master medium must be a Master A.
- A Master A can grant permissions to Master Bs. See section "Create A/B structure."
- A Master A can revoke permissions from Master Bs. See section "Delete Master Bs from the component"
- An INI reset can be initiated with a Master A, see section "INI reset with Master media"

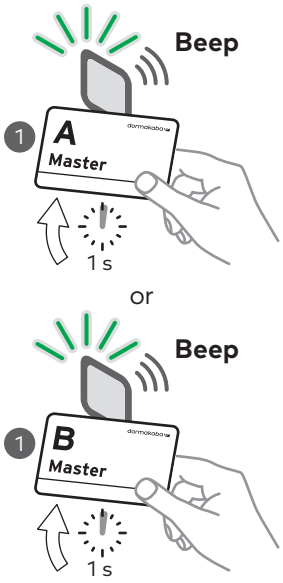
B structure

- In a B structure, the highest Master medium must be a Master B.
- An INI reset can be initiated with a Master B, see section "INI reset with Master media"

Prerequisites

- The component has factory settings assigned, see INI reset.

Procedure

	Hold Master medium (A or B) up to the antenna for approx. **1 second**. -> Glows green. -> 1 short signal sounds. -> Green goes out. -> The upstream Master medium has been registered as the highest Master medium.	1x short

7.4.1.2 Create A/B structure

After holding up the Master A, the component receives the following temporary permission:

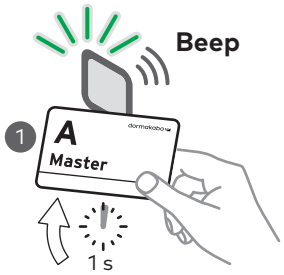
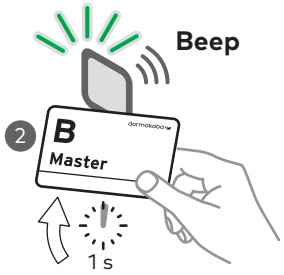
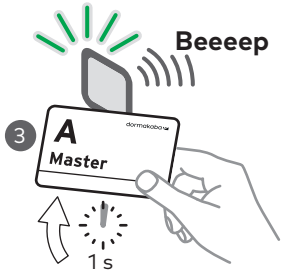
- Grant the Master B held up the permission to assign access permissions to user media.

After holding up the Master A again, the temporary permission for the component is revoked.

Prerequisites

- The Master A held up is the highest medium of the component.
  See section "Define highest Master medium"

Procedure

	Hold Master A up to the antenna for approx. **1 second**. -> Glows green. -> 1 short signal sounds. -> Green goes out.	1x short
	If no medium is held up for 20 seconds, the process is automatically terminated: -> The changes have been applied and 1 long signal sounds.	
	Hold Master B up to the antenna for approx. **1 second**. -> Glows green. -> 1 short signal sounds. -> Green goes out. -> Master B has the permission to assign access permissions to user media. -> The A/B structure has been created.	1x short
	If needed, hold up other Master Bs.	
	Hold Master A up to the antenna for approx. **1 second**. -> Glows green. -> 1 long signal sounds. -> Green goes out.	1x long

7.4.1.3 Grant access permissions

After holding up the Master B, the component receives the following temporary permission:

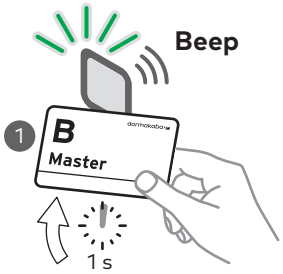
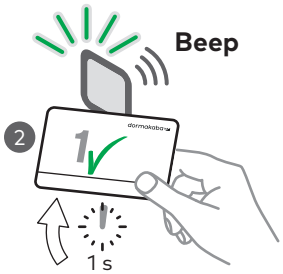
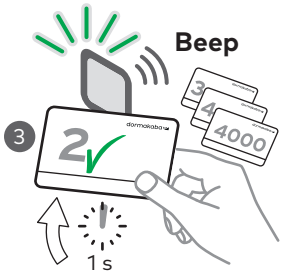
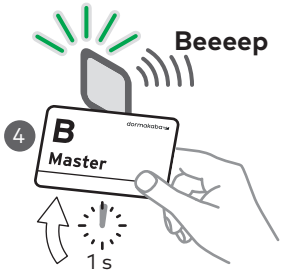
- Grant access permissions to the user medium held up (enter it on the whitelist).

After holding up the Master B again, the temporary permission for the component is revoked.

Prerequisites

- A/B structure or
- B structure is present

Procedure

	Hold Master B up to the antenna for approx. **1 second**. -> Glows green. -> 1 short signal sounds. -> Green goes out.	1x short
	If no medium is held up for 20 seconds, the process is automatically terminated: -> The changes have been applied and 1 long signal sounds.	
	Hold user medium up to the antenna for approx. **1 second**. -> Glows green. -> 1 short signal sounds. -> Green goes out. -> The user medium has been added to the whitelist. The user medium has access to the component.	1x short
	If needed, add other user media to the whitelist: Repeat step 2.	1x short
	Hold Master B up to the antenna for approx. 1 second. -> Glows green. -> 1 long signal sounds. -> Green goes out. -> The changes have been applied.	1x long
	If needed, grant access permissions with another Master B.	

7.4.1.4 Revoke individual access permissions

After holding up the Master B, the component receives the following temporary permission:

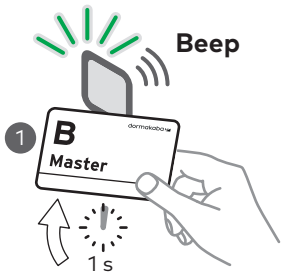
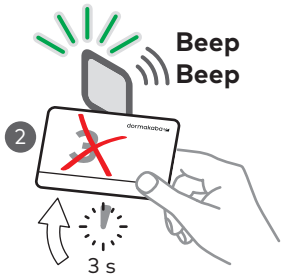
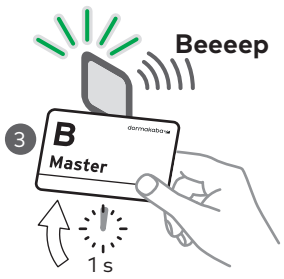
- Revoke access permissions from the user medium held up (remove it from the whitelist).

After holding up the Master B again, the temporary permission for the component is revoked.

Prerequisites

- User medium with access permission.
- A/B structure or
- B structure is present

Procedure

	Hold Master B up to the antenna for approx. **1 second**. -> Glows green. -> 1 short signal sounds. -> Green goes out.	1x short
	If no medium is held up for 20 seconds, the process is automatically terminated: -> The changes have been applied and 1 long signal sounds.	
	Hold user medium up to the antenna for approx. **3 seconds**. -> Glows green. -> 2 short signals sound. -> Green goes out. -> The user medium has been removed from the whitelist. The user medium does not have access to the component. If needed, hold up other user media.	2x short
	Hold Master B up to the antenna for approx. 1 second. -> Glows green. -> 1 long signal sounds. -> Green goes out. -> The changes have been applied.	1x long

7.4.1.5 Delete Master Bs from the component

After holding up the Master A, the component receives the following temporary permissions:

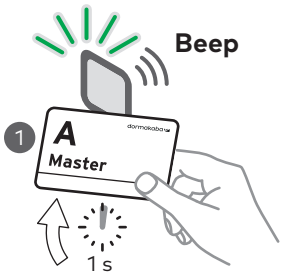
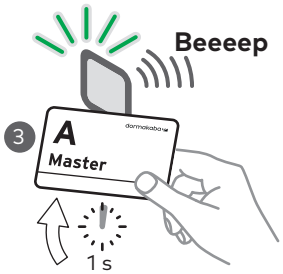
- Revoke all access permissions granted by the Master B held up (remove from the whitelist.)
- Revoke the permission to grant access permission from the Master B held up.

After holding up the Master A again, the temporary permissions for the component are revoked.

Prerequisites

- The Master B receives its permission through the Master A
- A/B structure is in place

Procedure

	Hold Master A up to the antenna for approx. **1 second**. -> Glows green. -> 1 short signal sounds. -> Green goes out.	1x short
	If no medium is held up for 20 seconds, the process is automatically terminated: -> The changes have been applied and 1 long signal sounds.	
	Hold up Master B to the antenna (approx. 10 seconds) until 2 short signals sound. -> Green glows as long as Master B is held up. If needed, hold up other Master Bs.	2x short
	Hold Master A up to the antenna for approx. **1 second**. -> Glows green. -> 1 long signal sounds. -> Green goes out. -> The changes have been applied.	1x long

7.4.1.6 Revoke all access permission assigned by Master B

After holding up the master B, the component receives the following temporary right:

- Cancel all access authorisations granted by the master B (remove from the whitelist).

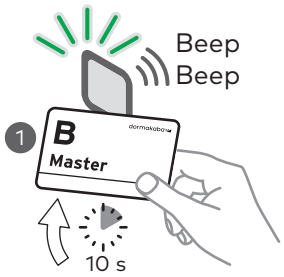
Note: The master B has the right to grant access authorisations.

Procedure

NOTICE

Data loss

If the master B is presented for **15 seconds**, the INI reset is initiated.
The INI reset deletes all the settings and data saved in the component.

	Hold master B up to the antenna for approx. **10 seconds**. -> Green glows. -> 1 long and 1 short signal sound (firmware version 42 and above). -> (pre-firmware version 42: 2 short signals sound.) -> Green goes out. -> All access rights assigned by the master B have been cancelled.	Firmware version 42 and above: 1 x long 1 x short
		Pre-firmware version 42: 2 x short

7.4.2 Key

7.4.2.1 Define highest Master medium

- The highest Master medium is the highest medium of a component.
- Each component must be assigned 1 highest Master medium.
- Each component can only be assigned 1 highest Master medium.
- The first Master medium that is inserted into the cylinder will be registered as the highest Master medium.

A/B structure

- In an A/B structure, the highest Master medium must be a Master A.
- A Master A can grant permissions to Master Bs. See section "Create A/B structure."
- A Master A can revoke permissions from Master Bs. See section "Delete Master Bs from the component"
- An INI reset can be initiated with a Master A, see section "INI reset with Master media"

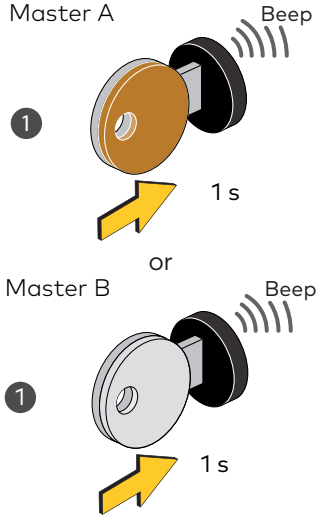
B structure

- In an B structure, the highest Master medium must be a Master B.
- An INI reset can be initiated with a Master B, see section "INI reset with Master media."

Prerequisites

- The component has factory settings assigned, see INI reset.

Procedure

	Insert Master medium (A or B) into the cylinder for approx. **1 second**. -> 1 short signal sounds. -> The upstream Master medium has been registered as the highest Master medium.	1x short

7.4.2.2 Create A/B structure

After inserting the Master A, the component receives the following temporary permission:

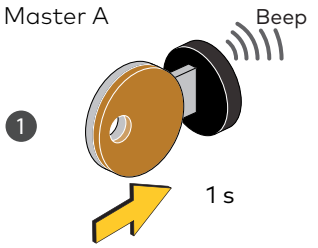
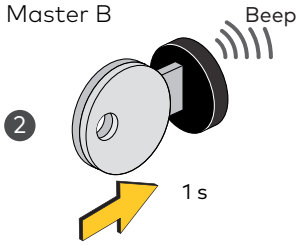
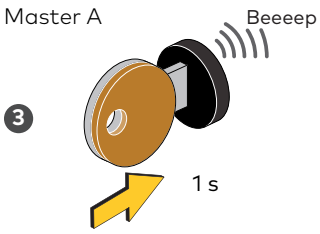
- Grant the Master B inserted into the cylinder the permission to assign access permissions to user media.

After re-inserting the Master A, the temporary permission for the component is revoked.

Prerequisites

- The Master A inserted into the cylinder is the highest medium of the component.
  See section "Define highest Master medium"

Procedure

	Insert the Master A into the cylinder for approx. **1 second**. -> 1 short signal sounds.	1x short
	If no medium is inserted into the cylinder for 20 seconds, the process is automatically terminated: -> The changes have been applied and 1 long signal sounds.	
	Insert Master B into the cylinder for approx. **1 second**. -> 1 short signal sounds. -> Master B has the permission to assign access permissions to user media. -> The A/B structure has been created.	1x short
	If needed, hold up other Master Bs.	
	Insert the Master A into the cylinder for approx. **1 second**. -> 1 long signal sounds.	1x long

7.4.2.3 Grant access permissions

After inserting the Master B, the component receives the following temporary permission:

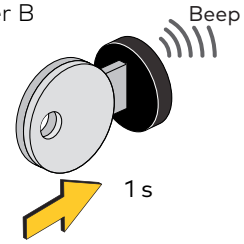
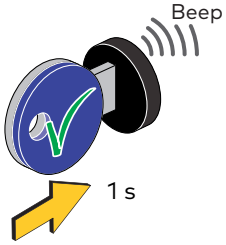
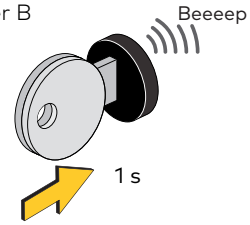
- Grant access permissions to the user medium inserted into the cylinder (enter it on the whitelist).

After re-inserting the Master B, the temporary permission for the component is revoked.

Prerequisites

- A/B structure or
- B structure is present

Procedure

Master B Beep 1 	Insert Master B into the cylinder for approx. **1 second**. -> 1 short signal sounds.	1x short
	If no medium is inserted into the cylinder for 20 seconds, the process is automatically terminated: -> The changes have been applied and 1 long signal sounds.	
User 1 Beep 2 	Insert user medium into the cylinder for approx. **1 second**. -> 1 short signal sounds. -> The user medium has been added to the whitelist. The user medium has access to the component.	1x short
User 2,3 ... Beep 3 	If needed, add other user media to the whitelist: Repeat step 2.	1x short
Master B Beeeep 4 	Insert Master B into the cylinder for approx. 1 second. -> 1 long signal sounds. -> The changes have been applied.	1x long
	If needed, grant access permissions with another Master B.	

7.4.2.4 Revoke individual access permissions

After inserting the Master B, the component receives the following temporary permission:

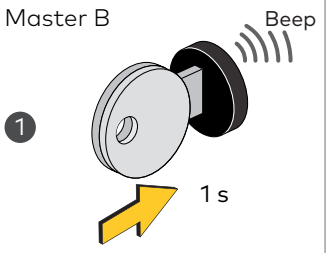
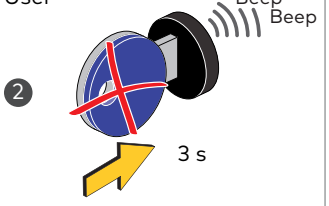
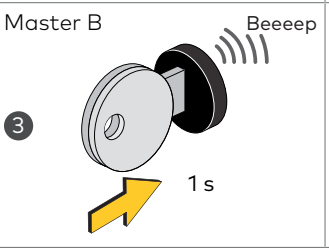
- Revoke access permissions from the user medium inserted into the cylinder (remove it from the whitelist).

After re-inserting the Master B, the temporary permission for the component is revoked.

Prerequisites

- User medium with access permission.
- A/B structure or
- B structure is present

Procedure

Master B Beep  	Insert Master B into the cylinder for approx. **1 second**. -> 1 short signal sounds.	1x short
	If no medium is inserted into the cylinder for 20 seconds, the process is automatically terminated: -> The changes have been applied and 1 long signal sounds.	
User Beep Beep  	Insert user medium into the cylinder for approx. **3 seconds**. -> 2 short signals sound. -> The user medium has been removed from the whitelist. The user medium does not have access to the component. If needed, hold up other user media.	2x short
Master B Beeeep  	Insert Master B into the cylinder for approx. 1 second. -> 1 long signal sounds. -> The changes have been applied.	1x long

7.4.2.5 Delete Master Bs from the component

After inserting the Master A, the component receives the following temporary permissions:

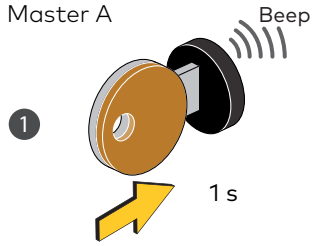
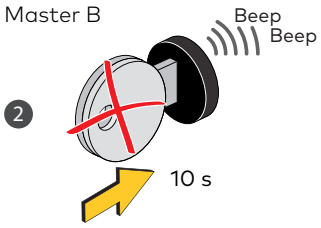
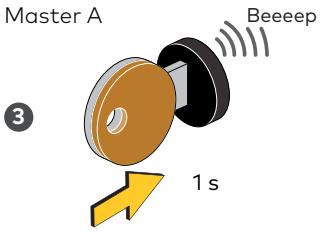
- Revoke all access permissions granted by the Master B inserted (remove from the whitelist.)
- Revoke the permission to grant access permission from the Master B inserted.

After re-inserting the Master A, the temporary permissions for the component are revoked.

Prerequisites

- The Master B receives its permission through the Master A
- A/B structure is in place

Procedure

Master A  	Insert the Master A into the cylinder for approx. **1 second**. -> 1 short signal sounds.	1x short
	If no medium is inserted into the cylinder for 20 seconds, the process is automatically terminated: -> The changes have been applied and 1 long signal sounds.	
Master B  	Insert Master B into the cylinder (approx. 10 seconds) until 2 short signals sound. If needed, hold up other Master Bs.	2x short
Master A  	Insert the Master A into the cylinder for approx. **1 second**. -> 1 long signal sounds. -> The changes have been applied.	1x long

7.4.2.6 Revoke all access permission assigned by Master B

After the master B is inserted, the component receives the following temporary right:

- Cancel all access authorisations granted by the master B (remove from the whitelist).

Note: The master B has the right to grant access authorisations.

Procedure

NOTICE

Data loss

If the master B is plugged in for **15 seconds**, the INI reset will start.
The INI reset deletes all the settings and data saved in the component.

Master B Beep Beep 1 10 s	Insert the master B into the cylinder for approx. **10 seconds**. -> 1 long and 2 short signals sound (firmware version 42 or above). -> (pre-firmware version 42: 2 short signals sound.) -> All access rights assigned by the master B have been cancelled.	Firmware version 42 and above: 1 x long 1 x short
		Pre-firmware version 42: 2 x short

7.4.3 INI reset with Master media

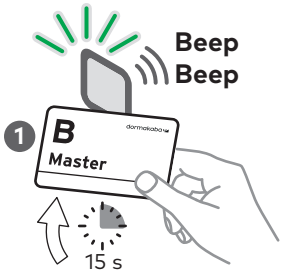
Consequences of an INI reset

- All parameter settings and data are deleted and returned to their original default values (factory settings).
- The access point is blocked during the INI reset.
- All access permissions, Master media and traceback are deleted.
- The passage is locked after the INI reset.

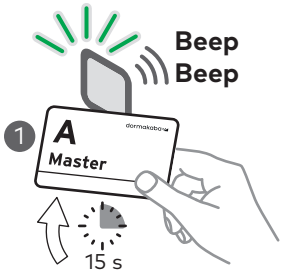
7.4.3.1 Cards

7.4.3.1.1 Whitelist

In Master B structure

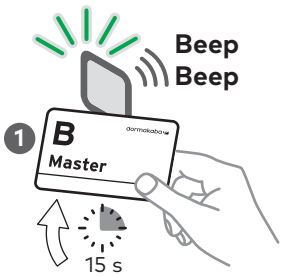
INI reset with Master B		
	Hold Master B up to the antenna for approx. **15 seconds**. -> Glows green. -> Successive signals sound. -> After 15 seconds the INI reset is carried out. -> Green goes out.	After 10 seconds: 1x long, 1x short, after 15 seconds, 2x short

In Master A/B structure

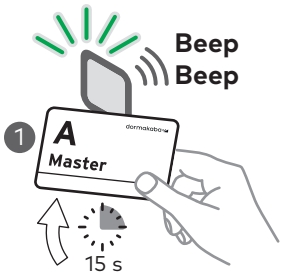
INI reset with Master A		
	Hold Master A up to the antenna for approx. **15 seconds**. -> Glows green. -> Successive signals sound. -> After 15 seconds the INI reset is carried out. -> Green goes out.	After 10 seconds: 1x long, 1x short, after 15 seconds, 2x short

7.4.3.1.2 Cardlink

With Master B

INI reset with Master B		
	Hold Master B up to the antenna for approx. **15 seconds**. -> Glows green. -> After 15 seconds the INI reset is carried out. -> 2 short signals sound. -> Green goes out.	2x short

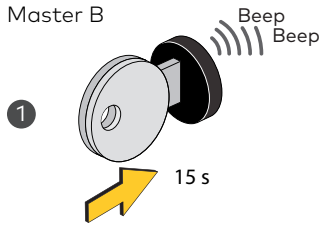
With Master A

INI reset with Master A		
	Hold Master A up to the antenna for approx. **15 seconds**. -> Glows green. -> After 15 seconds the INI reset is carried out. -> 2 short signals sound. -> Green goes out.	2x short

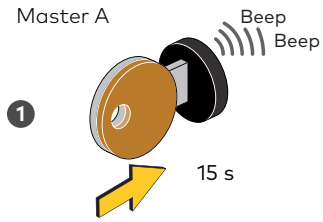
7.4.3.2 Key

7.4.3.2.1 Whitelist

In Master B structure

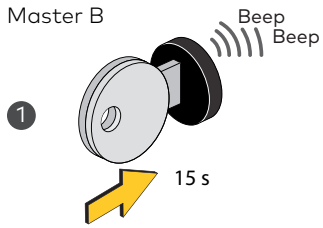
INI reset with Master B		
	Insert Master B into the cylinder for approx. **15 seconds**. -> Successive signals sound. -> After 15 seconds the INI reset is carried out.	after 10 seconds: 1x long, 1x short, after 15 seconds, 2x short

In Master A/B structure

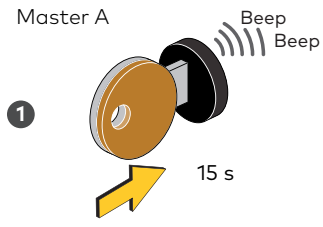
INI reset with Master A		
	Insert the Master A into the cylinder for approx. **15 seconds**. -> Successive signals sound. -> After 15 seconds the INI reset is carried out.	after 10 seconds: 1x long, 1x short, after 15 seconds, 2x short

7.4.3.2.2 Cardlink

With Master B

INI reset with Master B		
	Insert Master B into the cylinder for approx. **15 seconds**. -> After 15 seconds the INI reset is carried out. -> 2 short signals sound.	2x short

With Master A

INI reset with Master A		
	Insert the Master A into the cylinder for approx. **15 seconds**. -> After 15 seconds the INI reset is carried out. -> 2 short signals sound.	2x short

7.5 Programming with system software

With this programming type, the data that have been configured in the system software are transferred to the components with the programmer or via wireless. The master media of the master key system are an obligatory requirement for this programming type. In wireless operation, the master media are needed to put the components into operation. Programming of time functions and reading the traceback (event memory) are possible with this programming type.

With the system software, components and media are administered and authorizations are assigned. When this is done, a large number of organizational, structural and personal matters can be mapped and all the movements can be traced back.

7.5.1 System software for evolo components

Depending on the application and site size, different system software is used.

7.5.2 Programming with system software and programmer

Procedure

- Configure the device in the system software.
- Transmit the configuration to the programmer.
- Hold the master medium up to the antenna for approx. 1 second.
- Connect the programmer to the device.
- Transmit the configuration from the programmer to the device.

See also:

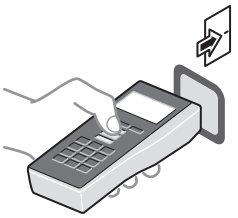
- System description
- Documentation for the system software used
- Programmer 1460 user manual
- Planning guidelines for wireless

7.5.3 Export to components

During the export, the configuration data is transferred from the programmer to the components.

For an export, configuration data for the key plans must first be transferred from the system software to the programmer.

7.5.3.1 Export to evolo components



Select the configuration data from the list in the programmer and export them to the components.

✓ Valid master medium available

1. Press the 'Export' menu key.
   ⇨ The 'Export' menu opens.
2. Log the master in to the component.

Activate the electronics on cabinet lock 21 10 by pressing briefly on the door.

3. Choose a key plan.
4. Press the ENTER key.
5. Choose an actuator.
6. Press the ENTER key.

7.5.4 Import from components

Activate the electronics on cabinet lock 21 10 by pressing briefly on the door.

When importing, the configuration data is transferred from the components to the Programmer. The programmer is then connected to a PC in order to further process the data with a host system, for example, in traceback analysis, or to create a support package that helps Support with error analysis.

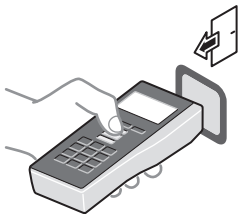
The following data is available for selection:

- Information (status data)
- Traceback
- Configuration
- CardLink update
- Diagnosis data

Existing configuration data of components is overwritten following confirmation on the programmer.

The traceback and the configuration must be transferred to the system software for evaluation with the Programmer.

7.5.4.1 Import from digital cylinder, c-lever and reader



✓ Valid master medium available

1. Press the 'Import' menu key.
   ⇨ The 'Import' menu opens.
2. Log the master in to the component.

Activate the electronics on cabinet lock 21 10 by pressing briefly on the door.

3. Choose a menu, e.g. 'Configuration'.
4. Press the ENTER key.

⇨ The component configuration is read and confirmed.

7.6 Mobile Access

7.6.1 System requirements

Firmware/System software

Function	Firmware	System software		
		Kaba exos 9300	**MATRIX**	**KEM**
Mobile Access	See section Validity > Mobile Access option	Version 4.0.73 or higher	MATRIX Professional Version 3.2.x or higher; with Mobile Access option MATRIX ONE Version 3.7 or higher	Version 6.0 or higher

7.6.2 Initialising the device for Mobile Access

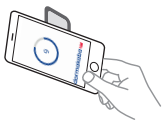
Prerequisites

General	• The access control system is set up by dormakaba for Legic Connect
System software	• The installed version of the system software supports Mobile Access. • A connection to Legic Connect has been established. • The device is configured in the system software for Mobile Access. • The configuration has been transmitted to the programmer.
Device	• The device is installed and ready for operation. • The media technology has been defined, see section “Define media technology” • The configuration has been transmitted from the programmer to the device.
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

Transfer the Bluetooth/NFC key to the device

- Hold the master medium up to the antenna for approx. 1 second.
- Start VCP Installer on the smartphone.
- Select the VCP file.
  - If the desired VCP file is not present, select “Update”. The smartphone will then download the VCP file .
- Tap on 'Send'.
- Input the password for the VCP file.



- Hold the smartphone in front of the reader.

Signal/display		
	Device/antenna	**Smartphone**
During data transmission:	• Green glows.	
After successful initialisation:	• Three signals are sounded.	• Green • Serial number of the device
The device is initialised.		
After unsuccessful initialisation:	• After a short acoustic signal, • Red glows briefly. • 1 long acoustic signal. • Red glows briefly.	• Red

Signal/display		
	Device/antenna	**Smartphone**
	• After a short acoustic signal,	

7.6.3 Initializing the device for evolo smart

The evolo smart app guides the user through the procedure for initializing components.

7.6.4 Set Bluetooth signal strength

Change the default values only if this is absolutely necessary.

- Devices without a wireless connection:
  In the parent system, set the Bluetooth signal strengths and transmit them to the device using the programmer.
- Devices with a wireless connection:
  In the parent system, set the Bluetooth signal strength and transfer it to the device via the wireless gateway.

Also see the Mobile Access planning guidelines

7.7 Initializing of wireless components

For the components to be operated wirelessly, wireless commissioning has to be carried out.

Additional information on wireless is given in the Wireless planning guidelines and in the technical manual for the Gateway 90 40 K7.

Requirements

- The relevant gateway is created and configured in the system software.
- The component is created in the system software.
- The component is configured for wireless operation.

For operation with multiple gateways, always start wireless commissioning on one gateway only.
The components could connect with an unwanted gateway.

Starting wireless commissioning on the gateway:
Via web interface

1. Select the gateway for commissioning the file manager.
2. Start the web interface of the gateway.
3. Call up the 'Wireless commissioning' function
4. Set the relevant period for commissioning.
   ⇨ The components can be connected to the gateway during this relevant period.
5. Start wireless commissioning.

Via system software

✓ The gateway for the putting into operation is created and configured in the system software.

1. In the system software, select the gateway for putting into operation.
2. Call up the 'Wireless commissioning' function
3. Set the relevant period for commissioning.
   ⇨ The components can be connected to the gateway during this relevant period.
4. Start wireless commissioning.

If it was not possible to commission all the necessary components within the relevant period set, the process can be repeated. Components already connected to the gateway remain connected.

Connect the component

✓ The gateway is created.

✓ The wireless configuration of the component has been transferred to the programmer or the component is already configured for wireless operation.

✓ Wireless commissioning on the gateway has started.

1. Log in to the component with the master medium.
2. Open the 'Actuator Settings' menu in the programmer.
3. Choose the 'Wireless' sub-menu.
4. Choose **Connect**.
5. Confirm with ENTER.
   - ⇨ Search for network... (Network is searched for.)
   - ⇨ Gateway (GW) found.
   - ⇨ Connecting to the GW is executed.
   - ⇨ Putting into operation...
   - ⇨ Connected to GW.

⇨ The wireless commissioning of the device is complete.

7.8 Setting the properties and functions of a component

The following properties of a component can be changed with the programmer:

- The date and time of the clock
- The acoustic signal and the visual display
- The opening time (default 6 s)
- The firmware version
- The INI reset
- Connecting a wireless component with a wireless gateway.

Main functions
The two main functions that can be performed on components with the Programmer are **export** and **import** of data. Both functions are performed with the Programmer via the radio interface (NFC) or with the programming cable.

7.9 Reset (INI reset)

With an INI reset, the components can be restored to factory settings.

NOTICE

Data loss

With an INI reset, all the settings and data stored so far on the E-module are deleted.

In the case of wireless components, the connection to the gateway is disconnected.

The following options are available for this purpose:

Reset with master media
An INI reset is executed when the respective master medium is held up to the components' registration unit.

With Programmer 1460
An INI reset can also be carried out with the programmer. For this variant, the respective master medium is also required.

Reset with tweezers and valid master media
Some components have INI reset contacts on the e-module. Short-circuit these contacts with a pair of electrically conducting tweezers and an INI reset is executed.

Reset with DIP switch
Some components have DIP switches. Switch on the specific DIP switch and an INI reset is executed.

Additional information on the INI reset is described in the documentation of the component.

7.9.1 Overview of INI reset variants for components

The INI reset variants and the differences for E300 (V4) and V3 are shown in the following table.

Some components have INI reset contacts. Short-circuit these contacts with a pair of electrically conductive tweezers for about 3 seconds, and an INI reset is executed.

Component	Admin master	Programmer 1460[1]	Tweezers	DIP switch
c-lever	✓	✓	✓	—
c-lever pro	✓	✓	✓	—
c-lever pro TouchGo	✓	—	✓	—
c-lever compact	✓	✓	—	—
Digital cylinder	✓	✓	✓ [2]	—
Mechatronic cylinder Forend	✓	✓	—[4]	—
Mechatronic cylinder Surface-fixed/ Compact	✓	✓	✓ [2]	—
Remote reader	✓	✓	—	✓ [3]
Compact reader	✓	✓	—	✓ [3]
Cabinet lock 21 10	✓	✓ [2]	✓	—

Legend:

1 Hold the master medium in front of it.

2 Hold the master medium or authorized user medium in front of it.

3 Set DIP switch 6 to ON.

4 Reset points in the forend module

Reset information for other components is described in the manuals of the components.

Always perform an INI reset in accordance with the device manual.

7.10 Saving energy

Standalone components
The amount of battery power and the energy consumption of standalone components determine how long they can operate before the energy reserve is exhausted. Energy can be saved through various setting options.

7.10.1 Deactivate functions

Deactivate functions not required to save energy.

Depending on the device type and its use, one or several functions can be disabled if they are not required for the intended use. This helps to save energy and extend the time between two battery changes.

Examples of functions that can be disabled:

- Acoustic signalling (acoustic signal generator)
- Visual signalling (illumination unit)
- Media traceback
- Technologies that are not required
- Wireless function (if not required)
- Reduce wireless transmitting power, if possible.
- Mobile Access (if not required)

7.10.2 'Object in Field' function

The component checks at regular intervals whether a medium is within the field of the antenna. To save energy, the relevant period between two checks can be extended. With a dynamic 'Object in Field', this relevant period is gradually extended to the maximum value. If a medium is held up, the process starts again. A longer reaction time is possible when holding up a medium.

The 'Object in Field' (OIF) function is parameterised in the system software.

Table: Saving energy through dynamic OIF. The values are approximate values. Actual energy saved still depends on other factors and settings.

Application	**Settings**		**Energy saved**	**Effects**
Examples	**OiF Interval**	**Dyn. OiF**	**Maximum**	
Default setting of component. **Highly frequented access points**	300 ms	OFF	0%	Normal
Low frequented access points	300 ms	ON 30 min	15%	Extended reaction time when first holding up a medium after a long pause. Normal for other media within the set time.
• 20 operations in the morning and 20 in the evening within the set time. Between that time one operation per hour for 10 hours.	300 ms	ON 30 min	19%	
• One operation per hour for 10 hours	300 ms	ON 30 min	22%	
Rarely needed access points • Two operations in the morning and two in the evening within the set time. No operations between that time.	300 ms	ON 30 min	30%	Extended reaction time for first use after a long pause. • Reading out a held-up medium can take up to one second.
• Long rest periods between the operations • No operation for one or more days	1,000 ms	OFF	34%	

8 Signals

This chapter describes the two types of signal, their meaning and the respective messages.

Acoustic signals and visual indicators are output when media are detected by the component's antenna.
The signals and indicators for access authorisation can be activated or deactivated individually using the tool chain.

Symbols

Symbols		Description
		Acoustic signal
		Visual signal

8.1 Signal duration

When user media with access authorisation are presented, the following acoustic signals (beep) and visual indicators (LED) are emitted.

Signals/indicators	Duration	Duration
Beep/LED illuminates	very brief	40 ms
Beep/LED illuminates	brief	120 ms
Beep/LED illuminates	long	600 ms
Beep/LED illuminates	very long	3000 ms

8.2 Access authorisations

Components and media are initialized and programmed.

Operating notifications:

Meaning			Media
Authorized (open)	1 x short	1 x short green	User media
Unauthorized (do not open)	4 x short	4 x short red	User media
Authorized (close) [3]	1 x short	1 x short green 1 x long red	User media
Authorized (close) [2, 3]	1 x short 1 x long	—	User media

Legend:

[1] Signals and displays can be enabled or disabled with the tool chain (with the system software (for example KEM) and the programmer).

[2] Components without a visual display.

[3] Closing with authorized media or actuating the button (c-lever), such as, for example, for Office Mode, Escape Return and Pass Mode.

8.3 Pass lock (c-lever) authorisations

Meaning			Media
Activate	1 x long	—	User media

Meaning			Media
Deactivate (close)	1 x brief	—	User media
Status (open)	—	very brief orange every 3 s	User media

8.4 Escape return and pass mode (c-lever) authorisations

Meaning			Activity
Activate	1 x long	1 x very long orange (3 s)	Hold down button for 2 s
Deactivate (close)	1 x long	5 x very brief orange	Hold down button for 2 s
Authorised (close)	1 x brief	1 x brief green 1 x long red	User media
Status (open)	—	1 x very long orange (3 s)	Briefly press button
Status (not open)	—	5 x very brief orange	Briefly press button

8.5 Messages when using the security card C2

When the security card C2 is used, the following acoustic signals and visual displays are signalled.

Note: The write authorization is deleted with the INI reset.

Use of the security card C2:

Workflow			Media
Start: Initialisation of the component	1 x short	Green, as long as the master medium is within the field of the registration unit	Master A or Master B
Programming of the write authorization	—	Green, as long as the process has not finished	Hold security card C2 within the field of the registration unit for 15 seconds
End: Programming of the write authorization is completed	3 times briefly	—	—
Deletion of the write authorization of security card C2	3 times briefly	—	—

8.6 Programming messages

Messages during programming:

Workflow			Media
Start: Media to program	1 x short	The LED lights up when there are media within the field of the registration unit. It does not light	Master A and Master B
Confirmation of programmed media [2]	1 x short		Master A and Master B
Medium deleted [2]	After 3 sec. 2 x short		User media

Workflow			Media
All media deleted [2]	After 10 sec. [3] 2 x short	up when there is an audible signal.	Master B (in A/B structure)
	After 10 sec.[4] 1 x long 1 x short		
End: Media to program	1 x long		Master A and Master B
Error during programming	1 x long	1 x short red	
Error during programming [1]	2 x long	—	

Legend:

[1] Components without a visual display

[2] Only for whitelist operation without host system

[3] Pre-firmware version 42

[4] Firmware version 42 and above

8.7 Wireless

Meaning			Tool
Identification of the component [6]	1 x short	1 x long green 1 x short green	

Legend:

[6] The signals are repeated every 3 seconds until the process is completed.

8.8 Reset messages

Note: The write authorization is deleted with the INI reset.

Meaning			Tool
Confirms the reset	After 3 sec. 2 x short	—	Tweezers Short-circuit INI reset contacts
Confirms the reset (whitelist)	After 10 sec. 1 x long 1 x short After 15 sec. 2 x short		Master media
Confirms the reset (CardLink)	After 15 sec. 2 x short		Master media
Confirms the reset	2 x short		Programmer 1460

8.9 Error and fault messages

Meaning			Media
Battery “Low” FW 42.XX	1 x very short	9 x very short red[3]	User media Master A and Master B
Battery “Low” FW 42.XX[1]	9 x very short[3]	—	User media Master A and Master B
Battery "Empty"	1 x very long[3]	—	User media Master A and Master B
Self-test function could not be completed[5]	8 x short	8 x short red	User media
Unauthorized media[4].	4 x short	4 x short red	User media
Failure of the internal clock in the component [2]	1 x long 1 x short 1 x long	1 x short green	User media Master A and Master B
Not all the site keys could be created	1 x short 1 x long 1 x short	2 x short red	Master A and Master B (MIFARE)
Not all the site's keys could be created			Service media

Legend:

1 Components without a visual display.

2 Condition, the clock was previously set correctly.

3 Then, 1x short green and the component opens.

4 Battery “Low” is not signalled.

5 Function only for c-lever, mechatronic cylinder and digital cylinder.
Note: It is recommended that a status check be carried out at the corresponding components.

9 System maintenance

9.1 Maintenance schedule



NOTICE

Danger of damage to electronic components from electrostatic discharge.

If electronic printed circuit boards and components are handled incorrectly, damage may occur which leads to their complete breakdown or sporadic faults.

- When installing and repairing the product, the general ESD protective measures are to be observed.

Carry out the following activities to be able to run master key systems and components trouble-free over a long time.

Detailed information on maintenance measures is provided in the separate operating manuals of the respective components.



Information on waiting periods and life expectancies of parts or components can vary according to the stress and ambient conditions.
The specified values refer to an average stress.

Check

- Carry out a function check of the components as per the manual every 12 months.
- Checking and setting the time with the Programmer 1460 every 12 months.
  In wireless operation, synchronisation of the clock takes place via the wireless gateway.

Update
Execute a firmware update for adjusting the functionality annually or as required. Avoid different firmware statuses of a component of a site.

Replace the batteries
The tables that follow show the average intervals after which the batteries of the components should be replaced. The average life depends on the battery type and the ambient conditions. It is also dependent on the configuration used (whitelist/CardLink), the equipment (standalone/wireless) and the options that have been set (for example, acoustic signalling).

Check the battery status every 12 months. Replace the batteries if required.

- Ambient conditions: See battery manufacturer's specifications.
- Battery type: Lithium. Use only recommended battery types.

9.2 Battery life

The life of a battery as an energy source for standalone components depends on many factors.

- Quality variations of the battery manufacturer.
- The type of the functions of a component used.
- Number of used and/or combined functions of a component.
- Number of procedures within a certain relevant period, for example per day/week/month/year.
- Ambient conditions like temperature, atmospheric humidity etc.

The component warns of a low battery level with signals.

Examples for the battery life of the miscellaneous components:

Assumptions for the table:

- Average temperature 20 °C

- Standalone operation
- Access type whitelist
- Without acoustic signalling

Component	Actuations per workday	Interval
c-lever pro	Approx. 250	24 months
c-lever		
c-lever compact	Approx. 100	24 months
Digital cylinder	Approx. 100	12 months
	Max. 50	24 months
Mechatronic cylinder forend variant	Approx. 400	12 months
	Approx. 100	24 months
Mechatronic cylinder variants - Compact - Surface fixed	Approx. 50	24 months
Cabinet lock 21 10	Approx. 100	24 months

Batteries in TouchGo media:

Components	Battery type	Voltage	Type	Temperature range	Service life
Key fob	CR2450	3 V	Lithium	–20 to 65 °C	approx. 1 year
Wristband	CR2450	3 V	Lithium	–20 to 65 °C	approx. 1 year
Card holder	CR2430	3 V	Lithium	–20 to 65 °C	approx. 1 year

9.3 Buffer time for changing the batteries

For the battery change, it must be noted that there is only a short time available for the replacement before the settings of the clock in the components are lost (see the following table).

Note: Check the settings of the clock in the components after the battery change.

Buffer times:

Components	Buffer time
c-lever	< 60 s
c-lever pro	< 45 s
c-lever compact	< 45 s
Digital cylinder	< 45 s
Mechatronic cylinder • Forend • Compact • Surface-fitted	< 45 s
Cabinet lock 21 10	< 120 s

9.4 Opening if batteries become discharged

If all alarm messages have been ignored to the point where the batteries are fully discharged, the components can only be opened using the emergency power supply of the Programmer 1460.

A description of the emergency supply (emergency opening) can be found in the user manual of the Programmer 1460.

In the case of the digital cylinder and c-lever compact, the battery or batteries are on the exterior. After performing the replacement, inspect the component's clock using the Programmer 1460 or via wireless, and set it if needed.

The cabinet lock 21 10 does not have an emergency opening function when the battery is empty. If the battery is empty, the lock would have to be broken open.

- Replace the battery when the display shows "Battery empty".

9.4.1 Temporary emergency opening medium

The use of an emergency opening medium is possible from firmware version 42.36.

If the battery is empty and the configuration is lost, a temporary emergency opening medium can still be programmed manually. This allows the door to be opened once to change the battery. Use of the emergency opening medium is possible with

- c-lever
- c-lever pro
- MC cylinder

The emergency opening medium is programmed into the RAM memory of the component using the master medium and is only valid for 1 minute or until the next restart.

For information on signalling, see the Programming messages [▶ 8.6].

Requirements

- Battery low or battery empty with emergency power supply
- The master medium is available.
- The emergency opening medium is a site-specific user medium.
- Operation mode: Whitelist
- The whitelist is empty.

Procedure

1. Present the master medium.
   ⇨ Signalling at low battery power: Battery low, followed by start of programming mode
   ⇨ Signalling with emergency power supply: Start of programming
2. Present the user medium provided as the emergency opening medium.
   ⇨ Only 1 emergency opening medium is possible.
   ⇨ Saving is signalled.
3. Present the master medium.

⇨ At the end of the programming procedure, you have 1 minute to open the door with the emergency opening medium. After that, the medium is deleted from the memory.

9.5 Configuration and traceback

Correctly set values for date and time ensure current time management with the components.

Components that are connected to the system software via the wireless function are updated via the gateway (e.g. time, configurations). The traceback can be read with the system software.

In pure standalone operation, the configurations are transferred with the programmer and can also be changed with it (e.g. setting the time).
The traceback can be read with a programmer and transferred to the system software for evaluation.

Further steps are described in the user manual for Programmer 1460.

9.6 Firmware update for components

The firmware of components can be updated in the evolo subsystem.

The new firmware versions are transferred with the programmer or via wireless into the standalone components.

Note: Multi RFID (MRD) components with manual programming must be checked after a firmware update for manual programming with the corresponding media. If required, an INI reset should be carried out.

In the case of some components (reader in online operation), functions can be changed by a firmware update.



If there are read/write authorisations on the component, the following applies from component firmware 42.40 and Programmer firmware 01.36:
The read/write authorisations (launch data) are **not** deleted by the firmware update.
If the read/write authorisations are to be deleted, an INI reset must be carried out.

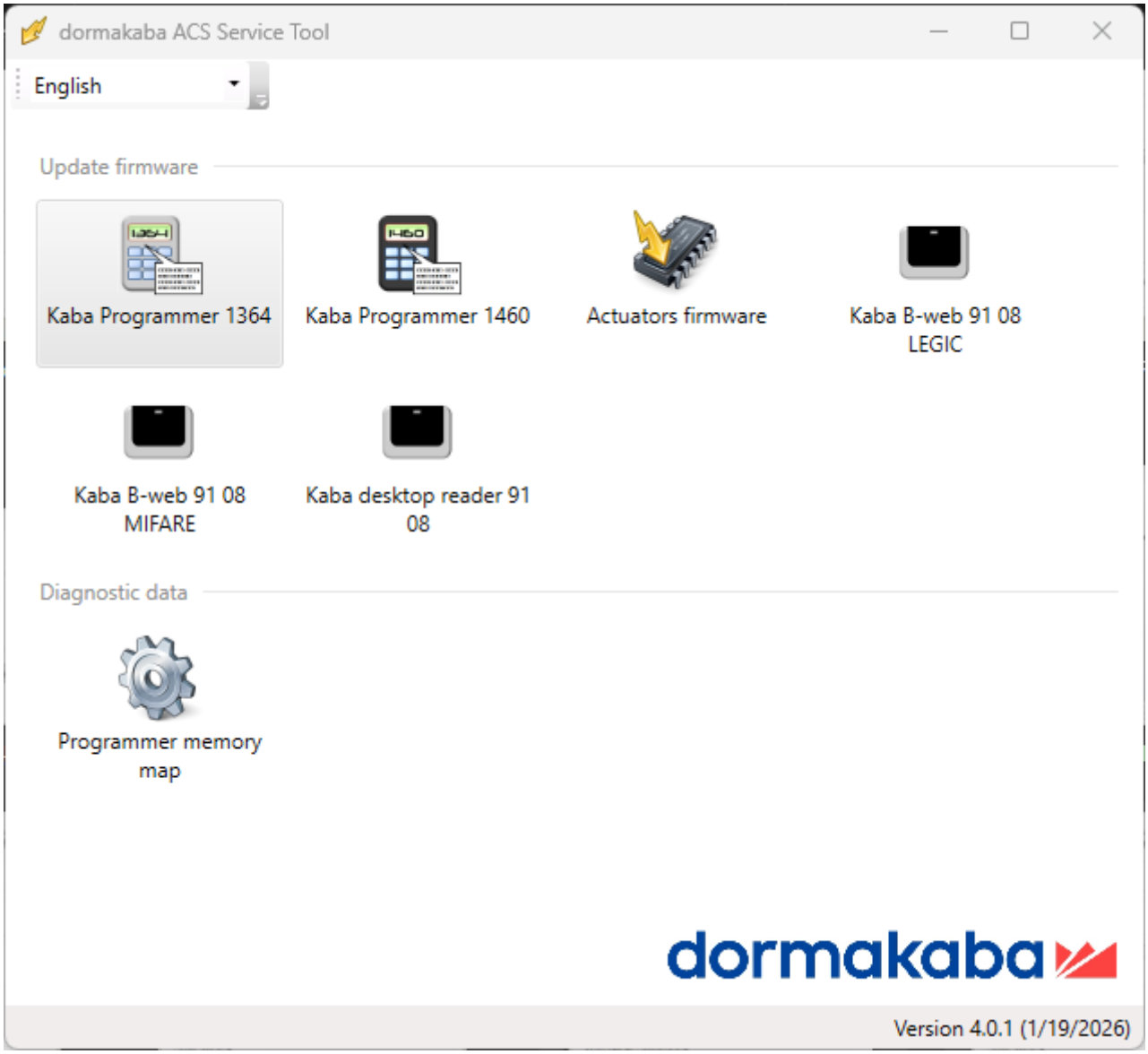
For a detailed description, see the user manual for the programmer 1460.

9.7 dormakaba ACS Service Tool

The dormakaba ACS Service Tool is an auxiliary program for updating firmware data and for conducting diagnoses.



You can also start the tool directly, that is, the system software does not need to be running. Navigate to *Start menu -> Programs -> Kaba -> dormakaba ACS Service Tool* to run it.



Programmer 1364	Wizard for updating the programmer firmware.
Programmer 1460	Wizard for updating the programmer firmware.
Actuators firmware	Wizard for transferring the firmware for the components to the programmer.
Desktop reader 91 08 LEGIC/MIFARE/MRD	Wizard for updating the desktop reader firmware for the selected technology.
Programmer 1460 memory image	Wizard for creating a ZIP file with the memory content of the programmer. A tool for problem-solving in support cases.

The firmware must be downloaded from the internet/extranet onto a local hard disk before updating.

Programmer 1364 is no longer available or supported. Latest downloadable firmware: 1.38

Notes

www.dormakaba.com

dormakaba Schweiz AG
Mühlebühlstrasse 23
8620 Wetzikon
Switzerland
T: +41 (0)44 931 61 11

www.dormakaba.com