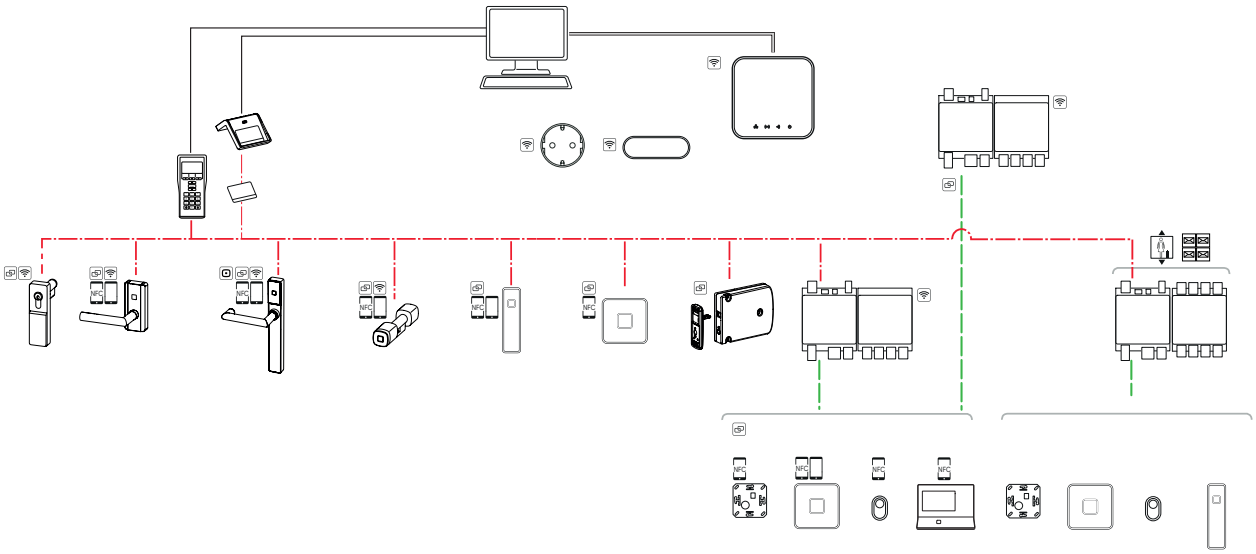
evolo Subsystem Beschreibung

Systembeschreibung



Public - 11/2026

DE

Inhaltsverzeichnis

1 Über dieses Dokument 5
1.1 Neue Funktionen und Aktualisierungen 5
1.2 Gültigkeit 5
1.3 Zielgruppe 5
1.4 Inhalt und Zweck 6
1.5 Verfügbarkeit der Dokumente 6
1.6 Ergänzende Dokumente 6
1.7 Abkürzungen / Begriffsdefinitionen 6
1.8 Warnhinweise 8

2 Übersicht 9
2.1 Berechtigung 9
2.2 Komponenten 9
2.3 Systemsoftware 11
2.3.1 Topologien 11
2.3.2 Toolkette 12
2.4 Smartphone-Zutrittsoptionen 13
2.4.1 Mobile-Access-Anwendungen 13
2.4.2 Wallet-basierter Zutritt (Apple Wallet und Google Wallet) 14
2.5 Medien 14
2.5.1 Master-Medien 17
2.5.2 Benutzermedien 18
2.6 Programmierstrukturen 19
2.6.1 A/B- und B-Struktur 19
2.7 OSS-SO-Unterstützung 20

3 Berechtigungsarten und Funktionen 22
3.1 Identifikationsnummer 22
3.2 Systemlevel 22
3.3 Whitelist-Berechtigung 23
3.3.1 Whitelist-Berechtigung mit Zeitprofil 24
3.4 CardLink-Berechtigung 26
3.4.1 Zutrittsrechte 26
3.4.2 Validierung 28
3.4.3 Validieren der Medien 28
3.4.4 Verlorene Medien 29
3.4.5 Blacklist 30
3.4.6 Servicemedien 30
3.4.7 Status Information 30
3.4.8 Medien Traceback 30
3.5 Access on Card 31
3.6 Mixed Mode 31
3.7 Unberechtigte Medien 31
3.8 TimePro-Funktionen 31
3.8.1 Office Zeitprofil 31
3.8.2 Day/Night Zeitprofil 33
3.9 Erweiterte Funktionen 33
3.9.1 Wireless Komponenten 33
3.9.2 Komponenten Traceback 36
3.9.3 S-Modul 36
3.9.4 Wiedereintrittsfunktion (Escape Return) bei c-lever pro 36
3.9.5 Pass-Mode bei c-lever pro 36
3.9.6 Pass-Lock bei c-lever pro 37
3.9.7 Interventionsmedien 37
3.9.8 Manuelles Programmieren deaktivieren 38
3.10 TouchGo 38
3.10.1 Funktionsweise RCID 38
3.10.2 Sicherheitsaspekte 38
3.10.3 TouchGo E110 39
3.10.4 TouchGo E310 39

3.11 Freie Schrankwahl beim Schrankschloss 21 10 und 21 20 40
3.12 Briefkasten/Aufzug 40

4 Systemvarianten 41
4.1 Whitelist Programmierung 41
4.1.1 Whitelist-Berechtigung ohne Toolkette 41
4.1.2 Whitelist-Berechtigung mit Toolkette 42
4.2 CardLink Programmierung 43
4.2.1 CardLink-Berechtigung über Tischleser 43
4.2.2 CardLink-Berechtigung über Update Reader 44
4.2.3 CardLink-Berechtigung über Terminal 45
4.3 Übersicht Firmware-Varianten 46

5 Sicherheitsfunktionen 48
5.1 Die Sicherheitsstufen LEGIC 48
5.2 Sicherheit mit CardLink-Berechtigungen LEGIC 48
5.3 Sicherheit mit der Whitelist-Berechtigung LEGIC 49
5.4 Die Sicherheitsstufen MIFARE 49
5.5 Sicherheit mit CardLink Berechtigungen MIFARE 50
5.6 Sicherheit mit der Whitelist Berechtigung MIFARE 50
5.7 Master T 51

6 Komponenten 52
6.1 Speichergrössen 52
6.2 Technische Daten 52
6.3 Master-Medien 55
6.4 Sicherheitskarten 55
6.5 Toolkette 56

7 Komponente Programmieren / Konfigurieren 58
7.1 Medientechnologie festlegen 58
7.2 Methoden zur Programmierung und Konfigurierung 58
7.3 TouchGo-Produkte programmieren 58
7.3.1 TouchGo E310 programmieren 59
7.3.2 Verlorene/defekte Benutzermedien 66
7.4 Programmieren mit Medien 67
7.4.1 Karten 68
7.4.2 Schlüssel 74
7.4.3 INI-Reset mit Master-Medien 79
7.5 Programmieren mit Systemsoftware 81
7.5.1 Systemsoftware für evolo Komponenten 82
7.5.2 Programmieren mit Systemsoftware und Programmer 82
7.5.3 Export in Komponenten 82
7.5.4 Import aus Komponenten 82
7.6 Mobile Access 83
7.6.1 Systemvoraussetzungen 83
7.6.2 Initialisieren des Geräts für Mobile Access 83
7.6.3 Initialisieren des Geräts für evolo smart 84
7.6.4 Bluetooth Signalstärke einstellen 85
7.7 Initialisieren von Wireless-Komponenten 85
7.8 Eigenschaften und Funktionen einer Komponente einstellen 86
7.9 Reset (INI-Reset) 86
7.9.1 Übersicht der INI-Reset-Varianten der Komponenten 86
7.10 Energie sparen 87
7.10.1 Funktionen deaktivieren 87
7.10.2 Funktion Object in Field 89

8 Signale 90
8.1 Signaldauer 90
8.2 Zutrittsberechtigungen 90
8.3 Berechtigungen Pass-Lock (c-lever) 90
8.4 Berechtigungen Escape Return und Pass-Mode (c-lever) 91
8.5 Meldungen bei Anwendung der Sicherheitskarte C2 91
8.6 Programmiermeldungen 91

8.7 Wireless 92
8.8 Resetmeldungen 93
8.9 Fehler- und Störungsmeldungen 94

9 Systempflege 95
9.1 Wartungsplan 95
9.2 Batterielebensdauer 95
9.3 Pufferzeit bei Batteriewechsel 96
9.4 Öffnung bei entladenen Batterien 96
9.4.1 Temporäres Notöffnungsmedium 97
9.5 Konfigurationen und Traceback 97
9.6 Firmware-Update von Komponenten 98
9.7 dormakaba ACS Service Tool 98

1 Über dieses Dokument

1.1 Neue Funktionen und Aktualisierungen

Die folgende Tabelle enthält die Verbesserungen in dieser Version des Subsystems, der zugehörigen Komponenten oder der Software/Firmware.

Änderung	Beschreibung	Einge-führt in
Pass-Lock-Aktivierungsverzögerung	Um eine unbeabsichtigte Aktivierung von Pass-Lock zu verhindern, kann eine Verzögerung konfiguriert werden. Der Taster muss während der gesamten konfigurierten Dauer gedrückt gehalten werden, bevor Pass-Lock aktiviert wird. Siehe Kapitel Pass-Lock bei c-lever pro [▶ 3.9.6].	42.48
Interventionsmedien	Es kann eine dedizierte Gruppe von Interventionsmedien definiert werden, die auch dann Zutritt behält, wenn Pass-Lock aktiv ist oder ein Einbruchdetektionssystem (IDS) scharf gestellt ist. Siehe Kapitel Interventionsmedien [▶ 3.9.7].	42.48
Google-Wallet-Unterstützung	Google Wallet kann an unterstützten evolo Komponenten über NFC als Benutzermedium verwendet werden. Siehe Kapitel Wallet-basierter Zutritt (Apple Wallet und Google Wallet) [▶ 2.4.2].	42.48
Apple-Wallet-Unterstützung	Apple Wallet kann an unterstützten evolo Komponenten über NFC als Benutzermedium verwendet werden. Siehe Kapitel Wallet-basierter Zutritt (Apple Wallet und Google Wallet) [▶ 2.4.2].	42.46
Access on Card (AoC): Option für unbegrenzte Gültigkeit	Bei Verwendung von MATRIX kann einem Benutzer eine unbegrenzte Zutrittsgültigkeit zugewiesen werden, wenn die betrieblichen Anforderungen des Kunden dies erfordern. Siehe Kapitel Access on Card [▶ 3.5].	42.40
Aktualisierte Bezeichnung des Wireless Gateway	Um den neuesten Verbesserungen Rechnung zu tragen, beschreibt dieses Handbuch das Wireless Gateway in seiner aktuellen Version **90 40-K7**.	-
c-lever air abgekündigt	Das Produkt wird Kunden nicht mehr angeboten und in diesem Handbuch nicht mehr erwähnt.	-

1.2 Gültigkeit

Das Dokument beschreibt das evolo Subsystem für die RFID-Technologien LEGIC, MIFARE und MRD (Multi RFID Device). Bei neuen Anlagen wird die MRD-Technologie eingesetzt.

Das Dokument beschreibt das evolo Subsystem für den Einsatz der Mobiltechnologien Bluetooth® und NFC.

Die Beschreibung umfasst Standalone-, Wireless-, Bluetooth®- und NFC-Komponenten.

Auf den Komponenten installierte Firmware-Version: ab Version 42.38

Beschreibungen oder Beispiele zur Verwendung der Komponenten mit Hostsystemen beziehen sich in diesem Handbuch auf die Verwendung mit KEM. Die Einbindung des evolo Subsystems in die Hostsysteme wird in den Dokumentationen der jeweiligen Hostsysteme beschrieben.

1.3 Zielgruppe

Diese Dokumentation richtet sich ausschließlich an Fachkräfte.

Die Beschreibungen setzen durch den Hersteller geschulte Fachkräfte voraus. Die Beschreibungen ersetzen keine Produktschulung.

Aus Gründen der Gerätesicherheit dürfen die in dieser Dokumentation beschriebenen Handlungen der Installation, Wartung und Instandhaltung nur durch Fachkräfte gemäß EN 62368-1 (Einrichtungen für Audio/Video-, Informations- und Kommunikationstechnik - Teil 1: Sicherheitsanforderungen) ausgeführt werden.

Fachkraft ist die Bezeichnung für Personen, die eine geeignete technische Ausbildung besitzen und Erfahrung mit der Technik der Einrichtung haben. Es wird erwartet, dass Fachkräfte ihre Schulung und Erfahrung anwenden, um Gefahren bei Ausführung der Handlungen für sich selbst und andere zu erkennen und möglichst gering zu halten. Es liegt in der Verantwortung der Fachkraft, dass die vom Hersteller genannten Bedingungen sowie geltende Vorschriften und Normen bei Ausführung dieser Handlungen eingehalten werden.

Diese Dokumentation dient auch zur Information für Personen mit folgenden Aufgaben:

- Projektplanung und Projektrealisierung
- Inbetriebnahme des Produktes innerhalb des Netzwerkes
- Anbindung des Produktes an die Anwendersoftware durch Programmierung von Kunden-Applikationen
- Kundenspezifische Anpassung durch Parametrierung des Produktes

1.4 Inhalt und Zweck

Dieses Dokument enthält die Grundlagen des evolo Systems und gibt einen zusammenfassenden Überblick.

1.5 Verfügbarkeit der Dokumente

Ergänzende Dokumentationen stehen unter folgendem Link zur Verfügung:

https://techdoc.dormakaba.com/cds

1.6 Ergänzende Dokumente

Die folgenden Dokumente sind über die Vertriebspartner verfügbar:

- Technische Dokumentation der eingesetzten Komponenten
- Handbuch Programmer 1460
- Dokumentation der eingesetzten Systemsoftware
- dormakaba evolo Produktkatalog

Option Touch Go

- Bedienungsanleitung dormakaba c-lever pro TouchGo
- Planungsrichtlinie dormakaba c-lever pro TouchGo mit S-Modul

Option Wireless

- Planungsrichtlinie Wireless

Option Mobile Access

- Planungsrichtlinie Mobile Access

1.7 Abkürzungen / Begriffsdefinitionen

Zur besseren Lesbarkeit werden die folgenden offiziellen Produktbezeichnungen durch Kurznamen ersetzt.

Produktbezeichnung / Definition	Kurzname
dormakaba evolo	evolo
dormakaba remote reader	Leser
dormakaba compact reader	

Produktbezeichnung / Definition	Kurzname
dormakaba digital cylinder	Digitalzylinder
dormakaba mechatronic cylinder, surface-fixed	Mechatronikzylinder
dormakaba mechatronic cylinder, compact	
dormakaba mechatronic cylinder, forend	
dormakaba terminal 94 20	Terminal
dormakaba c-lever pro TouchGo	TouchGo
dormakaba c-lever pro	c-lever
dormakaba c-lever compact	
Kaba c-lever	
dormakaba cabinet lock 21 10	Schrankschloss
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	Tischleser
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
Unikatsnummer	UID
Kartenidentifikationsnummer	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

Die folgenden Symbole stehen für akustische oder optische Signale:

Symbole		Signaltyp
		Akustisches Signal
		Optisches Signal

Bei Komponenten ohne optische Anzeigemöglichkeit entfällt die optische Signalisierung.

1.8 Warnhinweise

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt:



⚠ GEFAHR

Hohes Risiko

Bezeichnet eine unmittelbar drohende Gefahr, die zu schweren Körperverletzungen oder zum Tod führt.



⚠ WARNUNG

Mittleres Risiko

Bezeichnet eine möglicherweise gefährliche Situation, die zu schweren Körperverletzungen oder zum Tod führen kann.



⚠ VORSICHT

Geringes Risiko

Bezeichnet eine möglicherweise gefährliche Situation, die zu leichten Körperverletzungen führen kann.



ACHTUNG

Hinweise für den sachgerechten Umgang mit dem Produkt

Das Nichtbeachten dieser Hinweise kann zu Fehlfunktionen führen. Das Produkt kann beschädigt werden.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis der jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis vor Personenschäden gewarnt wird, dann kann im gleichen Warnhinweis zusätzlich vor Sachschäden gewarnt werden.

Weitere Warnsymbole:



Gefahr allgemein



Explosionsgefahr



Gefahr durch elektrische Spannung



ESD: Gefahr durch elektrostatische Entladung

Für den sicheren Betrieb des Produkts nützliche Hinweise und Informationen sind wie folgt gekennzeichnet:



Anwendungstipps, nützliche Informationen.
Sie helfen, das Produkt und dessen Funktionen optimal zu nutzen.

2 Übersicht

Das evolo Subsystem ist eine Menge aus standalone Komponenten, deren Konfiguration mit Hilfe der Toolkette übertragen wird.

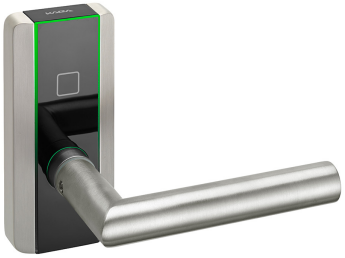
2.1 Berechtigung

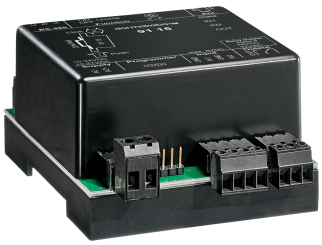
Beschreibung

Berechtigung	Beschreibung
Whitelist	Die Informationen der Berechtigung befinden sich in den Komponenten.
CardLink	Die Informationen der Berechtigung befinden sich in den Benutzermedien.
Access on Card AoC	Nur unter MATRIX verwendet: Die Informationen der Berechtigung befinden sich in den Benutzermedien. Weitere Informationen zu AoC befinden sich in der MATRIX-Dokumentation.
OSS-SO	Offener Standard. Weitere Informationen hier: http://www.oss-association.com/standards/oss-standard-offline/
Mobile Access	Bei Mobile Access wird das Smartphone zum Benutzermedium.

2.2 Komponenten

Elektronische Komponenten mit verschiedenen Funktionen, die in oder an Türen installiert werden können.

	Systemübersicht Komponenten	
Produktnummer	**Komponente**	**Beschreibung**
		c-lever pro **Optionen:** • Wireless • Mobile Access • OSS-SO • TouchGo E110 nur standalone, nicht für evolo Subsysteme kein Wireless • TouchGo E310 für evolo Subsysteme kein Wireless
		c-lever compact **Optionen:** • Wireless • Mobile Access • OSS-SO

	Systemübersicht Komponenten	
Produktnummer	**Komponente**	**Beschreibung**
143x / 153x		Digitalzylinder **Optionen:** • Wireless • Mobile Access • OSS-SO
21 20		Schrankschloss • OSS-SO
91 15	 	Remoteleser Gerät mit abgesetzter Erfassungseinheit **Optionale Erweiterungen:** • Wireless in Verbindung mit Erweiterungsmodul 90 43 (nicht abgebildet) • Mobile Access (Bluetooth mit entsprechender Erfassungseinheit) • OSS-SO • Gekoppelt mit dormakaba Kompaktleser-Subterminal 91 10

	Systemübersicht Komponenten	
Produktnummer	**Komponente**	**Beschreibung**
91 04	 	Kompaktleser **Optionen:** • Mobile Access nur NFC NFC und Bluetooth • OSS-SO • Gekoppelt mit dormakaba Kompaktleser-Subterminal 91 10
		Mechatronikzylinder **Optionen:** • Wireless • OSS-SO
		Lösung für Briefkastenzutritt/Aufzugsteuerung • Mobile Access

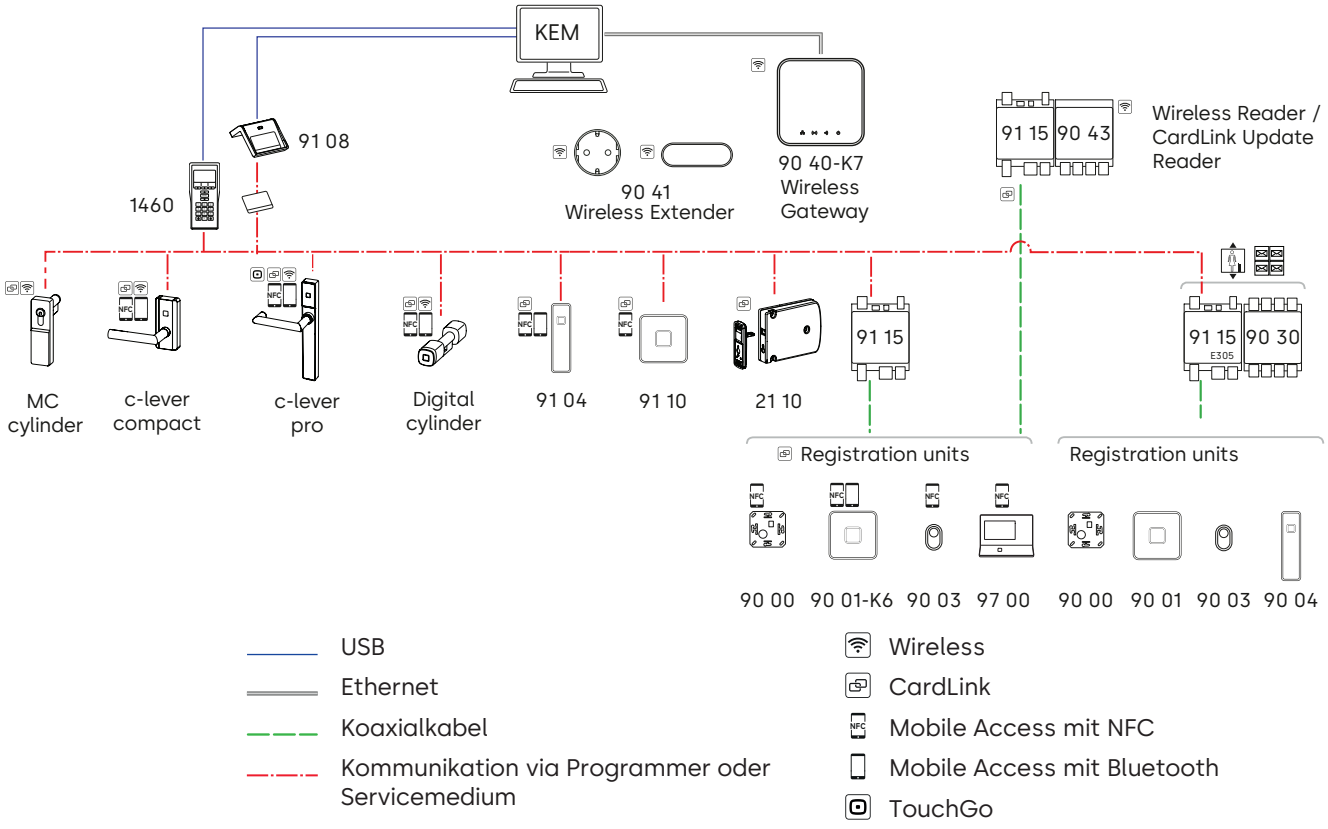
2.3 Systemsoftware

Die evolo Komponenten können außer mit dem dormakaba evolo Manager (KEM) auch mit anderer Systemsoftware konfiguriert werden.
Informationen zu den Möglichkeiten sind in der Dokumentation der verwendeten Systemsoftware beschrieben.

2.3.1 Topologien

Ein Beispiel einer möglichen Topologie.

evolo Komponenten unter KEM:
Stand: 03/2026



Legende				
90 00 90 01 90 03 90 04	Erfassungseinheit (Registration unit)		91 04 91 10	Kompaktleser
90 40-K7	Wireless Gateway		91 15 91 25	Remoteleser
90 41	Wireless Extender		90 30 90 43	Erweiterungsmodul
1460	Programmer		91 08	Tischleser B-web
91 15 + 90 30	Aufzug-/Briefkastensteuerung		91 15 + 90 43	Wireless-Leser Wireless-CardLink-Update-Leser

Die Planungsrichtlinien zu Wireless und Mobile Access enthalten weitere Informationen zu diesen Themen.

Mobile Access mit NFC: Mobile Access muss in der Komponente freigeschaltet sein.
Mobile Access mit Bluetooth: Die Komponente verfügt über die entsprechende Hardware für Bluetooth und Mobile Access ist in der Komponente freigeschaltet.

Siehe auch Kapitel [▸ 2.4.1]

2.3.2 Toolkette

Systemsoftware und Hardware zum Verwalten, Lesen und Schreiben der Berechtigung in Komponenten und Medien.

Systemübersicht Toolkette	
Tool	**Beschreibung**
	Tischleser 91 08 MRD Mit Systemsoftware und Tischleser werden Medien ausgelesen und beschrieben.

Systemübersicht Toolkette	
Tool	**Beschreibung**
	Programmer 1460 Das Gerät dient als Verbindungsglied zwischen den Standalone-Komponenten und der Systemsoftware. Das Gerät dient auch der Erstkonfiguration / Anbindung von Wireless-Komponenten an ein Wireless-Netzwerk.
	Wireless Gateway 90 40-K7 Das Gerät dient der Anbindung von Wireless-Komponenten an die Systemsoftware.
	Wireless Extender 90 41 Das Gerät vergrößert die Reichweite des Wireless Gateway.
	Wireless Reader Wireless-Anbindung für den Remoteleser 91 15 über ein angestecktes Wireless-Erweiterungsmodul 90 32. Für CardLink-Update über Wireless.
	Terminal Für CardLink-Update

2.4 Smartphone-Zutrittsoptionen

Als Alternative zu ihren üblichen Zutrittsmedien können Benutzer mobile Anwendungen oder den Wallet-basierten Zutritt nutzen. Einzelheiten sind in den folgenden Kapiteln beschrieben.

2.4.1 Mobile-Access-Anwendungen

In Mobile-Access-Anwendungen erfolgt der Zutritt mithilfe der Funktionen eines Smartphones. Mit Zutrittsberechtigung kann das Schloss/die Tür manuell geöffnet werden. Wenn der Zutritt gewährt wird, wird der Benutzer durch ein optisches und akustisches Signal informiert.

Die Konfiguration parallel zum konventionellen Zutritt mit Medien ist möglich.

Technische Voraussetzung für den vollen Funktionsumfang:

Um Bluetooth verwenden zu können, muss die Komponente mit der entsprechenden Hardware ausgestattet sein.

- Bluetooth-Fähigkeiten der Komponente mit Hilfe des Programmer überprüfen.

Technologie	Smartphone Betriebssystem	Komponente
NFC	Android	Standardausstattung und Mobile Access freigeschaltet

Technologie	Smartphone Betriebssystem	Komponente
NFC + BLE	Android IOS	Bluetooth-fähige Hardware und Mobile Access freigeschaltet

App	Beschreibung
mobile access App	Smartphone-App zum Öffnen von Türen. Benutzermedium
VCP Installer	Smartphone-App für die Inbetriebnahme von Türkomponenten (evolo Komponenten, Zutrittsleser).
evolo smart	Smartphone-App für die Inbetriebnahme und Verwaltung von Türkomponenten. Systemsoftware.

Systemsoftware

Die Systemsoftware [▶ 2.3] dient der Verwaltung des Schließplans. In den aktuellen Versionen kann Mobile Access im Schließplan konfiguriert werden. Siehe Kapitel Systemvoraussetzungen [▶ 7.6.1].

2.4.2 Wallet-basierter Zutritt (Apple Wallet und Google Wallet)

Apple Wallet und Google Wallet können an unterstützten evolo Komponenten als Benutzermedien verwendet werden. Der Zutritt wird über NFC gewährt, indem der Benutzer das Smartphone an die Komponente hält. Die dormakaba App ist für diese Funktion nicht erforderlich.

Der Wallet-basierte Zutritt ist unabhängig vom Bluetooth-basierten Mobile Access. Es ist keine zusätzliche Mobile-Access-Lizenz erforderlich, daher sind Komponenten der Produktlinien E300 und E320 ausreichend.

Voraussetzungen und Einschränkungen

- Die Firmware der Komponente muss Version 42.46 oder höher (Apple Wallet) bzw. Version 42.48 oder höher (Google Wallet) sein.
- Wenn in derselben Anlage MIFARE-Medien verwendet werden, ist MIFARE DESFire erforderlich. Wallet-Zutrittsdaten sind nicht mit MIFARE Classic kompatibel.
- Das Hostsystem muss die Funktion unterstützen. Informationen zur Konfiguration sind in der Dokumentation des jeweiligen Hostsystems beschrieben.

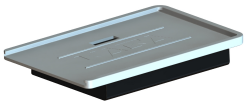
2.5 Medien

Master-Medien besitzen keine Zutrittsberechtigungen.

Systemübersicht Medien	
Medium	**Beschreibung**
Master-Medien	
	Master-A-Karte Mechatronik Zylinder Master A Schlüssel
	Master-B-Karte Mechatronik Zylinder Master B Schlüssel

Systemübersicht Medien	
Medium	**Beschreibung**
	Master-T-Karte (Verwendung nur bei KEM)
	TouchGo Master-Medium (RCID, nur TouchGo E110)

Die Benutzermedien werden mit der programmierten Zutrittsberechtigung an Türen und in Türgruppen eingesetzt.

Systemübersicht Medien	
Medium	**Beschreibung**
Benutzermedien	
	Karte
	Karte mit QR-Code (evolo smart)
	Mechatronik Zylinder
	Schlüsselanhänger
	Schlüsselanhänger mit QR-Code (evolo smart)
	Mobile Access Die Zugangsberechtigung erfolgt via Smartphone. In verschiedenen Anwendungen ist auch die Konfiguration der Komponenten via Smartphone möglich. Siehe Kapitel LINK [▶ 2.4.1]: Mobile Access Anwendungen
	TouchGo Schlüsselanhänger
	TouchGo Armband
	TouchGo Kartenhalter

Spezielle Medien:

Systemübersicht Medien	
Medium	**Beschreibung**
Sicherheitskarten	
	Die Sicherheitskarte wird für jede Schließanlage erstellt und dient der Anlagensicherheit. • MIFARE: Sicherheitskarte C • LEGIC: Sicherheitskarte C1 und C2
Wireless-Testmedium	
	Dies dient u.a. der Reichweitenmessung bei Wireless-Komponenten. Nur für Wireless-Komponenten. Weitere Informationen befinden sich in der Planungsrichtlinie Wireless.
Lizensierungskarten	
	Systemlevel-Upgrade Weitere Informationen befinden sich im Kapitel Systemlevel Kapitel [▶ 3.2].

2.5.1 Master-Medien

Mit den Master-Medien wird bei Standalone Komponenten der Programmiervorgang eingeleitet oder beendet.

Ohne Hostsystem:

- Nach der Einleitung des Vorgangs wird eine manuelle Whitelist konfiguriert.
  Siehe im Kapitel "Programmieren mit Medien"
- Die Master-B sind unter einem Master-A organisiert. Informationen zu den Programmierstrukturen befinden sich im Kapitel "Programmierstrukturen"
- Die Master-Medien besitzen keine Zutrittsberechtigung.

Mit Hostsystem:

Die Dokumentation des verwendeten Hostsystems enthält Informationen zur Verwendung der Mastermedien.

- Nach der Einleitung des Vorgangs wird mithilfe des Programmer eine Konfigurationsdatei geladen.
  Siehe "Programmieren mit Systemsoftware".

Wireless Komponenten:

- Ein Master-Medium wird benötigt, um mit dem Programmer die Verbindungsaufnahme der Komponente mit dem Wireless Gateway durchführen zu können.

Master T:
Die Master-T sind temporäre Master mit eingeschränkter Gültigkeit und eingeschränktem Funktionsumfang. Master T sind nicht in allen Hostsystemen möglich. Siehe Dokumentation des verwendeten Hostsystems.

TouchGo:
Der TouchGo E110 ist nur standalone Whitelist programmierbar und kann nicht mit einem Hostsystem eingesetzt werden. Zur Programmierung wird der RCID Master benötigt.

Der TouchGo E310 kann nur in einem evolo Subsystem mit Hostsystem und Toolkette verwendet werden. RCID und RFID Berechtigung werden in der Systemsoftware konfiguriert und an der Komponente durch Pairing verbunden. Das für das evolo Subsystem gültige Master-Medium wird verwendet.

Medien



TouchGo



RCID nur TouchGo E110

2.5.2 Benutzermedien

Mit den Benutzermedien wird den Benutzern ermöglicht, die erteilten Berechtigungen auszuüben und z. B. Türen zu öffnen.

Ohne Hostsystem
Bei der Whitelist-Programmierung werden die Benutzermedien unter einem Master-B organisiert.

ACHTUNG

Unberechtigter Zutritt mit verlorenem Medium

Verlorenes Medium aus Komponenten entfernen:

- Mit dem Master alle Zutrittsberechtigungen aufheben (aus der Whitelist entfernen), siehe Kapitel "Alle durch Master-B vergebenen Zutrittsberechtigungen aufheben".
- Den weiterhin gültigen Benutzermedien Zutrittsberechtigungen erteilen (in Whitelist eintragen), siehe Kapitel "Zutrittsberechtigungen erteilen".
- Das Vorgehen an allen Komponenten, an denen das verlorene Medium Zutritt hat, wiederholen.

Mit Hostsystem
Die Zutrittsberechtigungen der Benutzermedien werden mit Hilfe von Konfigurationsdateien programmiert. Informationen hierzu befinden sich im Kapitel "Programmieren mit Systemsoftware" [▶ 7.5.2].

Medien

RFID

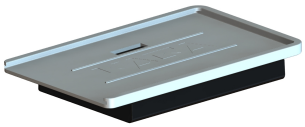


NFC/Bluetooth



TouchGo







Benutzermedium	RCID
Kombi-Medium	RCID + RFID

2.6 Programmierstrukturen

Nur bei standalone Programmierung ohne Hostsystem.
Nur Whitelist Programmierung.

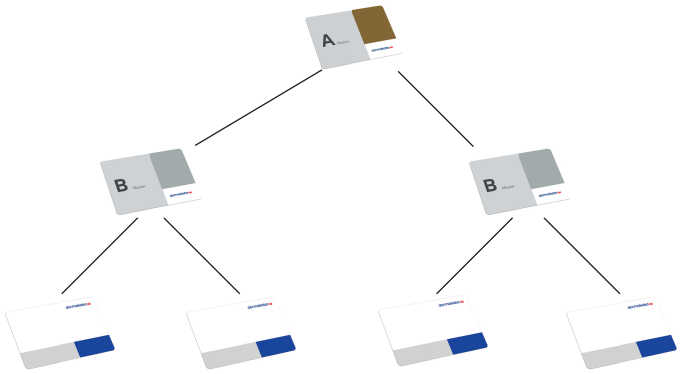
Organisation der Komponenten in einer A/B-Struktur oder in einer B-Struktur.

Die Programmierung wird im Kapitel "Programmieren mit Medien" beschrieben.

2.6.1 A/B- und B-Struktur

Karten-basierte Systeme:

A/B-Struktur

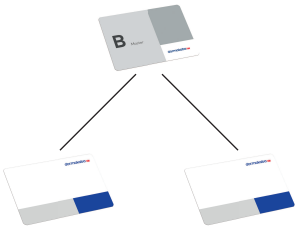


Master-A

Master-B

Benutzermedien

B-Struktur

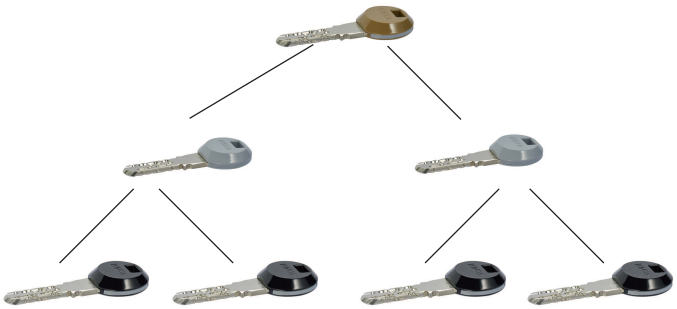


Master-B

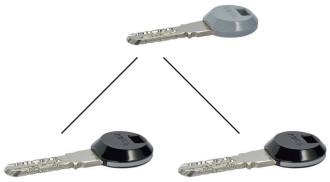
Benutzermedien

Mechatronik Systeme:

A/B-Struktur



B-Struktur



Beschreibung / Beispiele
A/B-Struktur:

Master-A:

- Maximal 200 Master-B anlegen
- Keine Programmierung der Benutzermedien
- Keine Programmierung von Zutrittsberechtigungen
- Weitere Anwendungen, siehe nachfolgende Kapitel

Master-B:

- Vergabe und Entzug von Zutrittsberechtigungen

Benutzermedien:

- Maximal 4000 Benutzermedien
- Die Verteilung der Benutzer auf verschiedene Master-B ist beliebig

Beispiel für 1 Komponente einer Anlage

- Master-B1: 50 Benutzer
- Master-B2: 3950 Benutzer

Summe = 4000: Maximale Anzahl Benutzer ist erreicht.

B-Struktur:

Master-B:

- Vergabe und Entzug von Zutrittsberechtigungen
- Weitere Anwendungen, siehe nachfolgende Kapitel

Benutzermedien:

- Maximal 4000 Benutzermedien
- Die Verteilung der Benutzer auf mehrere Master-B ist **nicht** möglich.

Beispiel für 1 Komponente einer Anlage

- Master-B: 4000 Benutzer

Summe = 4000: Maximale Anzahl Benutzer ist erreicht.

2.7 OSS-SO-Unterstützung

OSS-SO (Open Security Standards – Standard Offline) ist ein offener Industriestandard für die kartenbasierte Offline-Zutrittskontrolle. Er ermöglicht die Interoperabilität zwischen Zutrittskontrollsystemen und Offline-Schließgeräten verschiedener Hersteller. Die

Zutrittsberechtigungen werden auf dem Benutzermedium gespeichert (Data on Card) und direkt von der Komponente gelesen. Die Komponente muss nicht mit dem Hostsystem verbunden sein.

Die evolo Komponenten können unter OSS-SO eingesetzt werden. Die Konfiguration erfolgt mit der OSS-SO-Toolkette und den vom Hostsystem bereitgestellten XML-Dateien.

Einschränkungen
Die folgenden Funktionen werden beim Betrieb unter OSS-SO nicht unterstützt:

- S-Modul-Schaltfunktionen S-Modul [▶ 3.9.3]
- Pass-Mode Pass-Mode bei c-lever pro [▶ 3.9.5]
- Pass-Lock Pass-Lock bei c-lever pro [▶ 3.9.6]

Verhalten des Mechatronikzylinders im Office-Modus unter OSS-SO
Der Office-Modus wird am Mechatronikzylinder nicht unterstützt. Ist der Zylinder Teil einer Zutrittsgruppe, für die OSS-SO-Umschaltberechtigungen (Toggle) konfiguriert sind, führt die Komponente statt der Aktivierung des Office-Modus eine normale Öffnung aus. Dieses Verhalten entspricht dem Betrieb unter CardLink.

Weitere Informationen zu OSS-SO:

- http://www.oss-association.com/standards/oss-standard-offline/
- Referenzhandbuch OSS-SO XML-Datei
- Bedienungsanleitung der OSS-SO-Toolkette

3 Berechtigungsarten und Funktionen

Das Kapitel beschreibt die beiden Berechtigungsarten Whitelist und CardLink und die jeweiligen Funktionen der dazugehörigen evolo Komponenten.

- Whitelist: Siehe Kapitel
- CardLink: Siehe Kapitel
- AoC: Siehe Kapitel [▶ 3.5]

3.1 Identifikationsnummer

Den Medien und den Komponenten wird für die Berechtigung eine Identifikationsnummer vergeben. Diese wird zur eindeutigen Identifizierung benötigt.

Die Unikatsnummer (UID) ist eine eindeutige Identifikationsnummer, die vom Kartenhersteller vergeben und in den Benutzermedien abgelegt ist. Diese kann nicht geändert oder gelöscht werden.

Die Card ID (CID) ist eine eindeutige Identifikationsnummer, die über die Systemsoftware vergeben werden kann. Dies ist zur Zeit nur mit KEM möglich. Medien mit definierter CID können bestellt werden. Die CID ist mit dem einmaligen Anlagenschlüssel im Benutzermedium abgelegt und wird von den Anlagenkomponenten gelesen.

3.2 Systemlevel

Die Komponenten werden mit einem voreinstellten Systemlevel an den Kunden ausgeliefert. Der eingestellte Systemlevel bestimmt die Kopatibilität der Komponente zum verwendeten Hostsystem. Die Hostsysteme stellen die Konfiguration für den ihnen zugewiesenen Systemlevel bereit. Eine Komponente mit einem niedrigeren Systemlevel kann dann nicht konfiguriert werden. Eine Komponente mit einem höheren Systemlevel kann an einem Hostsystem mit einem niedrigeren Systemlevel verwendet werden.

Übersicht
Übersicht über die verwendeten Hostsysteme und den dazu passenden Systemlevel.

System	System level	Definition auf dem Programmer
		Firmware ab 1.30
evolo smart	SL1	1
MATRIX ONE/ exivo / KEM	SL2	2
MATRIX PRO / exos / EACM	SL3	3
OSS (3rd Party + dormakaba Host)	SL4	4

Der Systemlevel einer Komponente kann mithilfe des Programmer festgestellt werden.

Status Systemlevel und "BLE ready" feststellen.
Auf dem Programmer das Menü 'Aktuator Info' auswählen und die Informationen aus der Komponente auslesen.

Voraussetzungen:

- Programmer 1460
- Master-Medium der Komponente

Vorgehen:

1. Mit dem Master-Medium an der Komponente anmelden.
2. Das Menü Aktuator lesen auswählen.
3. Den Menüeintrag 'Info' auswählen.
4. Den Programmer mit der Komponente verbinden.

Die Firmwarevariante (E3xx) und Version feststellen.

Unter SL ist der Systemlevel angegeben.

Unter BLE zeigt ein Haken an, dass BLE aktiv ist.

Der Systemlevel wird ab den folgenden Versionen von den Komponenten und Hostsystemen unterstützt.

Die Komponente kann nur konfiguriert werden, wenn die Systemlevel von Komponente und Konfigurationsdatei übereinstimmen.
Die Komponente kann konfiguriert werden, wenn der Systemlevel der Komponente größer ist als der Systemlevel des Hostsystems (Gilt für SL1 bis SL3. Gilt nicht für SL4).

Ein Firmware-Update ist auch bei falschem Systemlevel möglich.

Host System	ab Version	Bemerkungen
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	Der Programmer vergleicht den Systemlevel der Parameterdatei mit dem Systemlevel der Komponente.
Komponente (Firmwareversion)	42.28	Im Werk wird der Systemlevel nach der Bestellung eingestellt.

Upgrade auf ein höheres Systemlevel
Die Komponenten werden ab Werk mit dem bestellten Systemlevel ausgeliefert. Wenn Funktionen verwendet werden sollen, die in diesem Systemlevel nicht freigeschaltet sind, dann muss der Systemlevel auf der Komponente auf den benötigten Stand gebracht werden. Hierfür können Upgrade Medien erworben werden.



Folgende Medien für Upgrade / Nachlizensierung werden angeboten:

Upgrade	SL1 zu SL2
Upgrade	SL2 zu SL3
Upgrade	SL1 zu SL3
Lizensierung	Mobile Access über BLE

Der Upgradevorgang ist im technischen Handbuch der Komponente beschrieben.

3.3 Whitelist-Berechtigung

Eine Whitelist-Berechtigung ist die Menge der in der Komponente eingetragenen Medien, die berechtigt sind.

Die Whitelist-Berechtigung wird in den Komponenten programmiert.
Das heißt, die UID oder die Card ID (CID) der zu berechtigenden Medien wird in den Komponenten gespeichert und somit in die Whitelist eingetragen.
In der Whitelist wird die UID oder die CID der präsentierten Medien verglichen. Wenn es

Übereinstimmungen gibt, sind die Medien berechtigt und die Komponenten öffnen. In der Whitelist sind bis zu 4'000 Einträge möglich. Es können die UID oder die CID eingetragen werden.

Funktionsbeispiel

Die Zutrittsberechtigung wird nur erteilt, wenn Benutzermedien präsentiert werden, deren UID oder CID in den Komponenten gespeichert sind.

Komponenten	Medien	Zutritt
Liste der in den Komponenten gespeicherten UID	**UID der präsentierten Medien**	
570AE209	570AE209	✓
222BE121	222BE121	✓
—	878EAE964	✗
—	121AC001	✗

3.3.1 Whitelist-Berechtigung mit Zeitprofil

Mit Zeitprofilen wird festgelegt, zu welchen Zeiten Medien an Komponenten berechtigt sind.

Alle evolo Komponenten besitzen eine eigene Uhr (Real Time Clock). Damit ist es möglich, den Benutzermedien zeitbezogene Zutrittsberechtigung pro Komponente und Tür zu erteilen.

Neben der grundsätzlichen Zutrittsberechtigung ist es mit Zeitprofilen möglich, eine Berechtigung zeitlich einzuschränken. Die Zeitprofile werden in der Systemsoftware festgelegt.

3.3.1.1 Whitelist-Berechtigung mit individuellem Zeitprofil

Insgesamt stehen pro Komponente 15 frei festzulegende Zeitprofile mit jeweils 12 Zeitfenstern zur Verfügung.

3.3.1.2 Whitelist-Berechtigung mit nicht veränderbarem Zeitprofil "Immer"

Dieses Zeitprofil hat den Zustand "Immer" und sichert die Öffnung während 24 Stunden, 7 Tage die Woche. Das Zeitprofil "Immer" kann nicht verändert, umbenannt oder gelöscht werden.

3.3.1.3 Ferien/Sondertage

Verfügbare Sondertage:

Zeitprofil V4	Verfügt über zwei Sondertage A und B

Hinweis: Wenn Komponenten mit dem Programmer 1460 aktualisiert werden, werden von der Systemsoftware immer die aktuellsten (von heute und in Zukunft) Ferientage und Sondertage übernommen.

Zeitprofile für Ferien

Für Perioden von aufeinander folgenden Tagen (z.B. Ferien) kann die Zutrittsberechtigung erteilt oder entzogen werden. Die Länge einer Periode wird mit der Eingabe von Start- und End-Datum festgelegt. Es können mehrere Ferienblöcke angelegt werden. In den Komponenten (V4) können insgesamt 20 Ferienblöcke definiert werden.

Hinweis zur Darstellung von Sondertagen innerhalb von Ferienblöcken: Befinden sich Sondertage innerhalb eines Ferienblocks, so werden diese in der Darstellung bevorzugt, d.h. die Darstellung des Ferienblocks wird durch die Darstellung des Sondertages überlagert. Wird der Sondertag entfernt, wird der Ferienblock wieder komplett angezeigt.

Zeitfenster für Sondertage

Für Sondertage (z. B. Feiertage) können 2 verschiedene Tage, Sondertag A und Sondertag B, angelegt werden. Damit ist es möglich zwei Zeitfenster anzulegen, z. B. ein Zeitfenster für einen Tag vor einem Feiertag (Sondertag A) und dem Feiertag (Sondertag B). Für jede der 2 Sondertagsarten können insgesamt 32 Sondertage in den Komponenten hinterlegt werden.

Sondertagsarten	Sondertag	Max. Anzahl Sondertage in der Komponente
Sondertag A	Tag vor einem Feiertag	32
Sondertag B	Feiertag	32

3.3.1.4 Sommer-/Winterzeit

In den Komponenten wird die Sommer-/Winterzeit Umstellung gemäß der eingestellten Welt-Zeitzone automatisch durchgeführt, abhängig von der eingesetzten Systemsoftware.

3.4 CardLink-Berechtigung

Bei der Berechtigungsart CardLink wird die Zutrittsberechtigung über die Benutzermedien verwaltet. Somit entfallen die lokalen Verwaltungsarbeiten an den Komponenten. Für diese Art der Berechtigung sind die Medienapplikationen auf den Benutzermedien notwendig.
Bei der Inbetriebnahme müssen die Komponenten einmalig programmiert werden.

Diese Berechtigungsart ermöglicht auch das Validieren (für eine bestimmte Zeit aktivieren – Validierung [▶ 3.4.2]) der Benutzermedien für die Zutrittsberechtigung an den standalone Komponenten.

Vorteile

- Die Zutrittsberechtigung wird direkt in die Benutzermedien geschrieben.
- Die Berechtigung kann in der Funktion **Reservation** zeitlich eingegrenzt werden.
- Einem Besucher kann eine individuelle Auswahl von Türen oder Türgruppen auf einem Benutzermedium zugewiesen werden.
- Bei zusätzlichen Benutzermedien ist keine weitere Konfiguration an den Komponenten notwendig.
- Durch das zusätzliche Anlegen von Gruppen wird der Aufbau der Schließanlagen und die Berechtigungsvergabe vereinfacht.

3.4.1 Zutrittsrechte

Den Benutzermedien wird eine einzelne, zeitlich begrenzte Berechtigung für eine Auswahl von Komponenten oder Türgruppen vergeben. Dazu wird in den Benutzermedien eine Liste von Türgruppen oder Türen gespeichert.

Türgruppen-Recht
Türgruppen-Rechte können organisatorisch (nach Personen) oder räumlich (nach Gebäudeteilen) zusammengefasst werden.

Ein Türgruppen-Recht ist eine Zutrittsberechtigung mit einem übergeordneten Zeitprofil. Für ein Türgruppen-Recht werden mehrere Personen oder Türen zu einer Türgruppe zusammengefasst. Die Türgruppe wird als Identifikation in den Komponenten gespeichert und der Türgruppe wird ein Zeitprofil zugewiesen. Anschließend kann den Benutzermedien diese Türgruppe zugewiesen werden, was den Zutritt zu allen in dieser Türgruppe zugeteilten Türen ermöglicht.
Für CardLink-Berechtigung stehen 15 Zeitprofile mit je 12 Zeitfenstern zur Verfügung, sowie das Zeitprofil "Immer", das immer gültig ist. Jeder Türgruppe kann ein entsprechendes Zeitprofil zugewiesen werden.

Anwendungen:

- Für große Schließanlagen mit vielen Benutzern und Türen. Mit der Konfiguration von Türgruppen kann die Schließanlage übersichtlich gestaltet und verwaltet werden.
- Für eine Personengruppe, die die gleiche Zutrittsberechtigung für eine Türgruppe erhalten sollen, wie die für Gruppenleiter und Hausdienste.

Einzelrecht
Ein Einzelrecht ist eine Zutrittsberechtigung mit einem individuellen Zeitprofil, das für eine einzelne Tür oder eine Türgruppe gültig ist.

Das Zeitprofil von einem Einzelrecht ist auf den Benutzermedien abgelegt. Bei einem Einzelrecht kann gegenüber der Türgruppe (Türgruppen-Recht) das Zeitprofil individuell ausgewählt werden.

Es stehen 2 Varianten zur Verfügung:

1 Einzelrecht für einzelne Türen
Für eine Tür können den Benutzermedien Zutrittsberechtigung mit individuellen Zeitprofilen zugewiesen werden.

2 Einzelrecht für Türgruppe
Für eine Türgruppe können einzelnen Benutzern (deren Benutzermedien) Zutrittsberechtigung mit individuellen Zeitprofilen zugewiesen werden.

Anwendungen:

- Für kleine Schließanlagen mit wenigen Benutzern und Türen.
- Für mehrere Benutzer, die individuelle Zutrittsberechtigung an einzelnen Türen erhalten sollen, wie die für Reinigungspersonal und Sicherheitskräfte.
- Für einzelne Benutzer, die individuelle Zutrittsberechtigung für eine Türgruppe erhalten sollen, wie die für Gruppenleiter und Hausdienste.

Reservation

Eine Reservation ist eine Zutrittsberechtigung für Besucher wie beim Einzelrecht, jedoch zusätzlich mit Start- und Enddatum oder Gültigkeitsdauer.

Anwendungen:

- Die Reservation ist eine temporäre Berechtigung und wird für Kunden, Besucher und Lieferanten eingesetzt.

Rechte-Priorisierung

Die Rechte sind priorisiert. Durch die Priorisierung der Rechte kann die Zutrittsberechtigung eines Mediums eingeschränkt oder ausgebaut werden.

Die Rechte werden in folgender Reihenfolge abgearbeitet.

- Einzelrecht
- Reservation
- Türgruppen-Recht

Die Auswertung des nachfolgenden Rechts wird nur weitergeführt, wenn kein “zeitlich falsches” Recht gefunden wird. Wird ein "zeitlich falsches" Recht gefunden, führt dies zu einem sofortigen Abbruch der Prüfung.

Innerhalb der Auswertung des Türgruppen-Rechts wird jedoch solange gesucht, bis:
a) alle Rechte kontrolliert sind oder, b) ein gültiges Recht (Türgruppe und passendes Zeitprofil) gefunden wird.

Funktionsbeispiel

Nachfolgend einige Beispiele für die verschiedenen Zutrittsrechte.

Die Bedingungen sind wie folgt:

- Türgruppe A --> Zeitprofil 1
- mehrere Komponenten --> Türgruppe A
- Tür “Eingang” --> Zeitprofil 1 bis 15

Beispiel Zutrittsrechte:

Zutrittsrechte	Medium mit Daten	Zutritt für	
		Türgruppe A	Tür "Eingang"
Türgruppen-Recht	Türgruppe A	✓ während Zeitprofil 1	✗
Einzelrecht der Türgruppe A	Türgruppe A + Zeitprofil 4	✓ während Zeitprofil 4	✗
Einzelrecht der Tür	"Eingang" + Zeitprofil 3	✗	✓ während Zeitprofil 3
Reservation der Türgruppe A	Türgruppe A + Zeitprofil 2 von Start bis Stopp	✓	✗

Zutrittsrechte	Medium mit Daten	Zutritt für	
		während Zeitprofil 2 Start bis Stopp	
Reservation der Tür	"Eingang" + Zeitprofil 7 von Start bis Stopp	✗	✓ während Zeitprofil 7 Start bis Stopp
Kombination zwischen Türgruppen-Recht und Einzelrecht	Türgruppe A "Eingang" + Zeitprofil 3	✓ während Zeitprofil 1	✓ während Zeitprofil 3

3.4.2 Validierung

Die Validierung (Zeitstempel auf den Benutzermedien) ist eine Aktivierung einer Zutrittsberechtigung. Der Zutritt ist nur mit einer gültigen CardLink-Berechtigung und der aktivierten Validierungsdauer [▶ 3.4.3] möglich.

Vorteile

- Verlorene Benutzermedien können schnell und einfach durch die Validierung gesperrt werden.
- Die CardLink-Berechtigung verfällt nach Ablauf der Validierungsdauer. Damit erlöschen die Zutrittsberechtigung und die Validierung. Die Validierung kann nicht mehr erneuert werden.

3.4.3 Validieren der Medien

Validierung mit standalone Komponenten

Die standalone Komponenten können auch als Validierungs-Komponenten eingesetzt werden. Die Validierungs-Komponenten können für die Validierung von CardLink-Berechtigung konfiguriert werden. Bei Änderung der Validierung müssen die Komponenten mit dem Programmer 1460 oder über Wireless aktualisiert werden.

Da die Validierung zusätzliche Energie benötigt wird empfohlen, hierfür nur Komponenten zu verwenden, die über eine externe Energieversorgung verfügen. Geeignet sind z.B. Remoteleser, Kompaktleser oder c-lever mit S-Modul.

Validierung mit Wireless Update Reader

Benutzermedien können an einem oder mehreren Wireless Update Reader validiert werden. Gleichzeitig kann die Validierung oder die Zutrittsberechtigung von verlorenen Benutzermedien dort entzogen werden. Die Validierungsdaten werden von der Systemsoftware verwaltet und über Wireless an den Update Reader übertragen.

Validierung mit Terminal

Benutzermedien können an einem oder mehreren Validierungs-Terminals validiert werden. Gleichzeitig kann die Validierung oder die Zutrittsberechtigung von verlorenen Benutzermedien direkt an einem Terminal entzogen werden. Das Terminal wird von der Systemsoftware verwaltet.

Validierungsdauer

Mit der Validierung an einem Validierungs-Terminal oder einer Validierungs-Komponente wird ein Zeitstempel auf die Benutzermedien geschrieben. Ab diesem Zeitpunkt ist die Zutrittsberechtigung für CardLink standalone Komponenten gültig.

Beim Präsentieren von Benutzermedien wird die Gültigkeitsdauer der Medien geprüft. Das heißt, dass der Zutritt nur dann erteilt wird, wenn die Gültigkeitsdauer nicht abgelaufen ist und die zeitliche Berechtigung für die entsprechende Türgruppe bzw. Tür (in Übereinstimmung mit dem Zeitprofil) vorhanden ist.

Die folgenden Validierungstypen sind einsetzbar:

Validierungstypen	Status
Dauer in Tagen und Stunden	In Tagen und Stunden. (max. Wert 999 d und 24 h)

Validierungstypen	Status
24 Stunden (1 Tag)	Der Typ ist nicht veränderbar.
Endtageszeit (h)	Bis zu einer bestimmten Tageszeit.
“Immer”	Der Typ ist nicht veränderbar.



Für den Validierungstyp “Immer” können verlorene Benutzermedien nicht mehr deaktiviert werden. Deshalb müssen verlorene Benutzermedien zwingend auf unbeschränkte Zeit in die Blacklist [▶ 3.4.5] der Komponenten eingetragen werden.
Der Speicherplatz zum Eintragen verlorener Medien in der Blacklist ist begrenzt.
Dieser Validierungstyp wird nicht zur Anwendung empfohlen.

Validierungsarten
Bei den Validierungsarten wird zwischen Medien-Typ und komponenten-Typ unterschieden. Die Art der Validierung wird immer an der Komponente eingestellt. In einer Schließanlage können beide Validierungsarten eingesetzt werden.

Medien-Typ (Standard)
Die Dauer der Validierung wird standardmäßig auf allen Benutzermedien angelegt. Beim Präsentieren von Benutzermedien an Komponenten wird der aktuelle Zeitstempel und Validierungs-Dauer der Benutzermedien gelesen und mit der aktuellen Zeit der Komponente verglichen. Ist die aktuelle Zeit früher als der Zeitstempel und die Dauer, ist die Validierung gültig. Ist die aktuelle Zeit später, gilt die Validierungszeit als abgelaufen und das Medium als ungültig.

Komponenten-Typ
Die Dauer der Validierung wird auf den Komponenten gespeichert. Beim Präsentieren von Benutzermedien an Komponenten wird nur der aktuelle Zeitstempel der Benutzermedien gelesen und mit der aktuellen Zeit der Komponenten verglichen. Ist die Zeit innerhalb der Validierungsdauer, ist die Berechtigung der Benutzermedien gültig. Ist die Zeit später, gilt die Validierungszeit als abgelaufen und das Medium ist ungültig und nicht mehr berechtigt.

Folgende Validierungsarten sind möglich:

Validierungsarten	Validierungsdauer bestimmt durch	Zu aktualisierenden Zeitstempel
Medien (Standard)	Medien	auf den Medien
Komponenten	Komponenten	auf den Medien

Funktionsbeispiel
In einer Schließanlage wird die Validierungszeit von 48 Stunden gewählt, die in den Benutzermedien gespeichert ist. Bei jedem Zutritt am Haupteingang werden die Benutzermedien aktualisiert und erhalten den Zutritt für die Türen im Gebäude. Mitarbeiter mit Auto benutzen den Parkplatz im Außenbereich, der mit einer Schranke gesichert ist. Da an der Komponente der Schranke nicht validiert werden kann, sind die Validierungen von 48 Stunden nach den Wochenenden oder Ferien nicht mehr gültig. Die Schranke würde geschlossen bleiben. Für diesen Fall kann die Schranke mit der Komponenten-Validierung konfiguriert werden. Diese ermöglicht es, eine Validierungsdauer von 4 Wochen einzustellen. Somit wird sichergestellt, dass die Schranke auch mit einem 3 Wochen alten Zeitstempel öffnet.

3.4.4 Verlorene Medien

Für verlorene Benutzermedien wird die Validierung nicht mehr erneuert. Dadurch werden diese Medien ungültig und der Zutritt gesperrt.

Es gibt 4 Möglichkeiten, um verlorene Medien auszuschließen:

- Bei Terminals wird das Medium in der Systemsoftware auf den Status “Verloren” gesetzt und anschließend vom Terminal nicht mehr validiert.
- Bei Validierungs-Komponenten wird das Medium in die Blacklist eingetragen. Das verlorene Medium kann nicht mehr validiert werden. Das Medium wird jedoch erst nach Ablauf der Validierungsdauer ungültig.
- Im Betrieb mit standalone Komponenten wird das Medium in die Blacklist eingetragen. Anschließend werden die Daten mit dem Programmer, einem Servicemedium oder, falls vorhanden, über wireless an alle standalone Komponenten der jeweiligen Anlage übertragen.

- Im Betrieb mit wireless Komponenten wird nach dem Austragen des verlorenen Medium in der Systemsoftware eine neue Parametrierung an die Komponenten übertragen.

3.4.5 Blacklist

Mit der Funktion Blacklist können Benutzermedien an allen standalone (Validierungs-) Komponenten gesperrt werden.

Müssen Benutzermedien innerhalb der Gültigkeitsdauer einer Validierung gesperrt werden, so ist diese Sperrung mit dem Programmer 1460 oder einem Servicemedium an allen standalone Komponenten der entsprechenden Anlage vorzunehmen. Anschließend kann die Rückbestätigung in die Systemsoftware mit dem Programmer 1460 oder dem jeweiligen Servicemedium übertragen werden.

Die Sperrung kann auch über die Toolkette Systemsoftware -- Programmer bzw. wireless erfolgen.

3.4.6 Servicemedien

Servicemedien sind nur unter KEM möglich.

Bevor Medien als Servicemedien eingesetzt werden können, müssen sie mit Hilfe der Systemsoftware als solche definiert werden. Hierfür stehen Funktionskarten, die mit eigenem Layout als solche identifizierbar sind, zur Verfügung.



Benutzermedien, die verloren gegangen sind, können mit der Systemsoftware in die Blacklist [▶ 3.4.5] eingetragen werden. Dieser Blacklist Eintrag wird auf das Servicemedium geschrieben und mit diesem an die Komponenten übertragen. Die Rückbestätigung erfolgt durch das Wiedereinlesen des Servicemediums in die Systemsoftware.

3.4.7 Status Information

Die Status Informationen sind zusätzliche Informationen, die von der Komponente auf die Medien übertragen werden. Wenn eine Komponente einen zu tiefen Batteriestand erreicht, wird diese Status Information auf die Medien geschrieben. Wenn Medien mit diesen Status Informationen von einem Tischleser oder einem Terminal ausgelesen werden, wird die Information an die Systemsoftware weitergeleitet und dort angezeigt.

Bei wireless Komponenten werden die Statusinformationen drahtlos an die Systemsoftware übermittelt und dort angezeigt. Der Vorgang muss gegebenenfalls in der Systemsoftware angestossen werden.

3.4.8 Medien Traceback

Die Funktion kann in der Systemsoftware konfiguriert werden.

In der Berechtigungsart CardLink besteht die Möglichkeit, medienspezifische Zutrittsereignisse auf den Benutzermedien zu speichern. Diese Daten können von einem Tischleser oder Terminal ausgelesen und an die Systemsoftware übertragen werden.

Zum Beispiel werden folgende Ereignisse und Zustände gespeichert:

- Zutritt mit Berechtigung
- Zutritt verweigert
- Validierung ungültig
- Falsche Zeit

3.5 Access on Card

Im Modus Access on Card (AoC) werden die Berechtigungen auf dem Benutzermedium gespeichert. Die Zutrittsdaten haben eine Gültigkeitsdauer, die je nach Bedarf des Benutzers variieren kann. Die Gültigkeitsdauer kann auch auf unbegrenzt gesetzt werden, d. h. ohne Ablaufdatum. Der AoC-Modus wird in der MATRIX-Umgebung eingestellt.

Bei Data on Card werden bei einer Buchung Daten der Komponente auf dem Benutzermedium gespeichert. Diese werden von einem an ein Hostsystem angeschlossenen Leser ausgelesen und im Hostsystem weiterverarbeitet.

3.6 Mixed Mode

Beim Mixed Mode werden auf einem Medium Cardlink oder Whitelist Berechtigungen gespeichert. Wird das Medium einer im Mixed Mode konfigurierten Komponente vorgehalten, überprüft die Komponente zuerst auf eine Whitelist-Berechtigung. Wird keine Berechtigung gefunden, dann wird auf Cardlink-Berechtigung geprüft. Die Komponente öffnet, wenn das Medium in einer dieser Berechtigungsarten berechtigt ist.

Wird das Medium in beiden Berechtigungsarten gefunden und das Medium ist in einer Berechtigungsart als "nicht berechtigt" eingestuft, dann wird das Medium abgewiesen.

Beispiel: Die Komponente öffnet nicht, wenn bei einem Medium eine gültige CardLink Berechtigung vorliegt, für das Medium aber auch eine WhiteList Berechtigung mit einem Zeitprofil ausserhalb der Gültigkeit vorliegt.

3.7 Unberechtigte Medien

Die Komponenten bleiben geschlossen, wenn unberechtigte Benutzermedien präsentiert werden. Wenn im geöffneten Zustand unberechtigte Benutzermedien präsentiert werden, bleiben die Komponenten geöffnet. Die Komponenten signalisieren die Ablehnung unberechtigter Medien.

3.8 TimePro-Funktionen

In diesem Kapitel werden die TimePro-Funktionen Office und Day/Night beschrieben.

Detaillierte und ergänzende Informationen über die beiden TimePro-Funktionen und deren Eigenschaften für die elektronischen Komponenten sind in der Betriebsanleitung der Systemsoftware KEM beschrieben.



Beim c-lever und c-lever pro können die TimePro-Funktionen und die folgenden Funktionen nicht miteinander kombiniert werden:

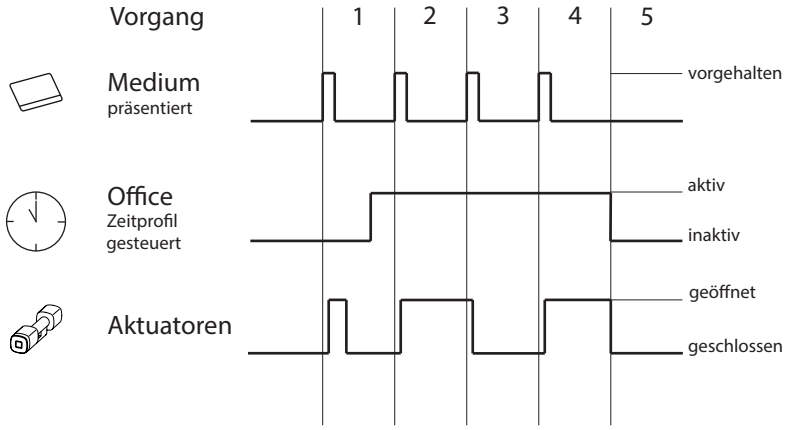
- Pass-Mode
- escape return

3.8.1 Office Zeitprofil

Innerhalb des eingegebenen TimePro-Zeitprofils können die Komponenten von berechtigten Medien in den geöffneten Zustand versetzt werden.

Hinweis: Die Funktion Office Zeitprofil kann in der Systemsoftware auf einzelne Benutzermedien beschränkt werden.

Funktionsbeispiel



Vorgang 1
Die geschlossenen Komponenten werden mit berechtigten Benutzermedien geöffnet. Nach einer bestimmten Öffnungszeit (von einigen Sekunden) schließen die Komponenten automatisch wieder.

Vorgang 2
Nach dem Präsentieren von berechtigten Benutzermedien bleiben die Komponenten dauerhaft geöffnet.

Vorgang 3
Wenn im geöffneten Zustand berechtigte Benutzermedien präsentiert werden, schließen die Komponenten wieder.

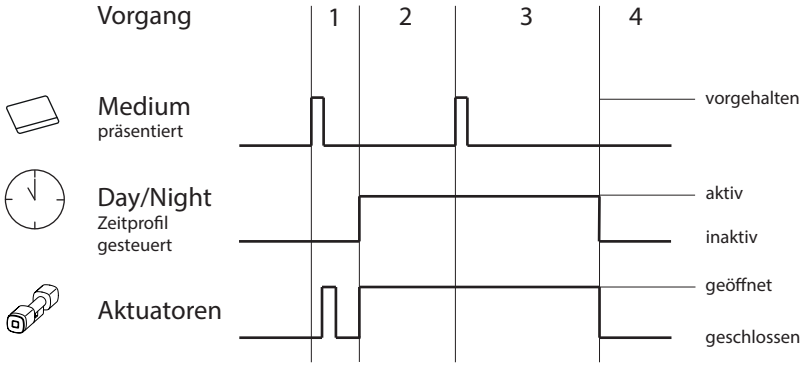
Vorgang 4
Nach dem erneuten Präsentieren von berechtigten Benutzermedien bleiben die Komponenten dauerhaft geöffnet.

Vorgang 5
Wenn das Office Zeitprofil abgelaufen ist, schließen die Komponenten automatisch.

3.8.2 Day/Night Zeitprofil

Mit dem Zeitprofil Day/Night wird der Zeitraum bestimmt, in dem sich die Komponenten im geöffneten Zustand befinden.

Funktionsbeispiel



Vorgang 1
Die geschlossenen Komponenten werden mit berechtigten Benutzermedien geöffnet. Nach einer bestimmten Öffnungszeit (von einigen Sekunden) schließen die Komponenten automatisch wieder.

Vorgang 2
Bei Start des Zeitprofils öffnen die Komponenten automatisch.

Vorgang 3
Während des geöffneten Zustands von Komponenten haben berechtigte bzw. unberechtigte Medien keinen Einfluss auf den Zustand der Komponenten. Die Komponenten bleiben geöffnet und signalisieren wie bei Medien mit Zutrittsberechtigung.

Vorgang 4
Nach dem Ablauf des Zeitprofils schließen die Komponenten automatisch wieder.

Funktionsbeispiel

Die Zutrittsberechtigung wird nur erteilt, wenn Benutzermedien präsentiert werden, deren UID oder CID in den Komponenten gespeichert sind.

Funktionsbeispiel Whitelist mit Zeitprofil:

Komponenten	**Medien**	**Zutritt**
Liste der in den Komponenten gespeicherten UID und dazugehörigen Zeitprofile	**UID der präsentierten Medien für eine bestimmte Zeit**	
	Bsp.: Freitag, 5. August 2014/ 10:15 Uhr	
578AE976 “Immer”	578AE976	✓
222BE121 Montag - Freitag 8:00 - 17:00	222BE121	✓
829FE649 Sonntag 10:00 - 12:00	829FE649	✗
—	121CA001	✗

3.9 Erweiterte Funktionen

3.9.1 Wireless Komponenten

Mit der wireless-Funktion werden die kabellosen standalone Komponenten V4 über Funk mit der jeweiligen Systemsoftware verbunden.

Die wireless-Funktion ist eine Option für die standalone Komponenten V4 (MRD), wie z.B. den Digitalzylinder und den elektronischen Beschlag c-lever. Die Option wird mit der Systemsoftware, z.B. KEM, konfiguriert.

Vorteile

- Weniger Administrations- und Verwaltungsaufwand
- Zutrittsberechtigung in Echtzeit ändern
- Ereignisse und Zustände direkt abfragen und speichern
- Batteriestatus anzeigen
- Firmware-Update via Funk übertragen

Einschränkungen sind:

- Die Funktion kann mit TouchGo nicht kombiniert werden.

3.9.1.1 Übersicht

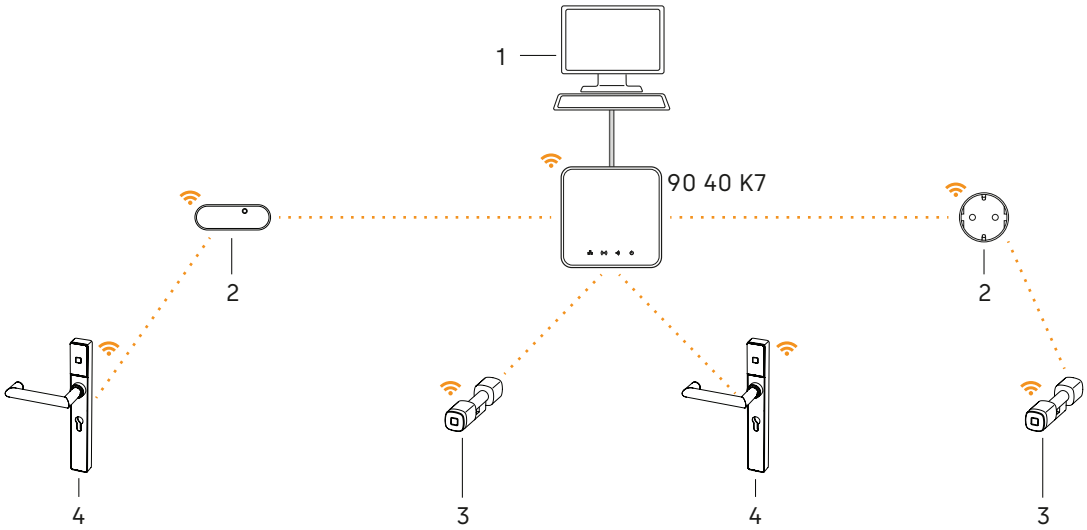
Über das Wireless Gateway werden Wireless-Komponenten an ein Zutrittskontrollsystem angeschlossen.

Das Zutrittskontrollsystem wird mit einer Systemsoftware verwaltet. Mit der Systemsoftware werden die angeschlossenen Geräte konfiguriert und die Zutrittsrechte vergeben.

Die Datenübertragung zur Systemsoftware erfolgt über die Ethernet-Leitung. Die Datenübertragung zu den Wireless-Komponenten erfolgt über Funk.

Die Reichweite der Funkverbindung kann mit Wireless Extender verlängert werden.

Topologie
Die Grafik zeigt die Einbindung des wireless Gateways in ein dormakaba System mit wireless Komponenten und wireless Extendern.



Wireless-Gerät
Wireless-Kommunikation

1 Übergeordnetes System
2 Wireless Extender
3 Wireless-Komponente (Digitalzylinder)
4 Wireless-Komponente (c-lever pro)

1 Systemsoftware
2 Wireless Gateway

3 Wireless Türkomponente

- Es können max. 16 Wireless Türkomponente an einem Wireless Gateway angeschlossen werden.

4 Wireless Extender

- Es können max. 8 Wireless Extender an einem Wireless Gateway angeschlossen werden.
- Es können max. 4 Wireless Extender hintereinander angeschlossen werden. (Wireless Gateway → 1. Wireless Extender→ ... → 4. Wireless Extender)

3.9.1.2 Messung mit dem Site Survey Tool

Mit dem Site Survey Tool lässt sich an verschiedenen Punkten die Signalqualität eines wireless Gateway messen. Mit Hilfe der Messergebnisse kann die Position des Gateway so bestimmt werden, dass alle wireless Komponenten mit einer optimalen Signalqualität erreicht werden. Ist die Signalqualität für den sicheren Betrieb nicht ausreichend, dann müssen weitere Gateways bzw. Extender zum System hinzugefügt werden.

Weitere Informationen befinden sich in der Planungsrichtlinie wireless und in der Programmbeschreibung zum Site Survey Tool.

3.9.1.3 Reichweitenmessung mit wireless Test-Medium

Alternative Messmethode, falls das Site Survey Tool nicht verfügbar ist.

Eine detaillierte Beschreibung der Reichweitenmessung mit dem Gateway ist in der separaten Anleitung PG Wireless (Planungsrichtlinie) und im Handbuch zum Wireless Gateway zu finden.

Notwendiges Medium: Wireless Testmedium



3.9.1.4 Inbetriebnahme

Die Inbetriebnahme der Wireless-Komponenten mit dem Programmer 1460 ist in den Handbüchern des Programmer, des Gateway und der Systemsoftware beschrieben.

Prinzip
Die Wireless-Inbetriebnahme wird auf dem Gateway 90 40-K7 gestartet, mit dem sich die Komponente verbinden soll. Mithilfe des Programmer wird an der Komponente die Verbindungssequenz eingeleitet. Wenn die Komponente erfolgreich mit dem Gateway verbunden ist, kann die Komponente online mit der Systemsoftware konfiguriert werden.

3.9.2 Komponenten Traceback

Das Komponenten Traceback ist eine Logbuch Datei, in die alle Ereignisse von Komponenten eingetragen und gespeichert werden. Die Funktion kann in der Systemsoftware deaktiviert werden.

Im Speicher werden bis zu 2'000 Ereignisse aufgezeichnet. Der neueste Eintrag überschreibt den ältesten Eintrag. Jeder Eintrag erhält einen Zeitstempel. Hierzu muss die Uhrzeit der Komponente korrekt eingestellt sein. Mit den Aufzeichnungen lässt sich jeder berechtigte oder verweigerte Zutritt zu einer Tür nachvollziehen.

Zum Beispiel werden folgende Ereignisse und Zustände gespeichert:

- Zutritt mit Berechtigung
- Zutritt verweigert auf Grund fehlender Berechtigung oder Validierung
- Zutritt verweigert auf Grund des falschen Zeitfensters
- Uhrzeit einstellen
- Programmierung
- Systemtest, usw.

3.9.3 S-Modul

Mit dem S-Modul wird das Verhalten der Komponente (Berechtigung) durch einen externen potentialfreien Kontakt übersteuert. Das S-Modul wird durch einen Schalter, Zeitschalter oder das Gebäudeleitsystem (z.B. Alarmanlage) aktiviert. Eine Komponente mit S-Modul kann über ein externes Netzteil mit Energie versorgt werden. Batterien werden in diesem Fall nicht mehr benötigt.

Das S-Modul ist für folgende Komponenten möglich:

c-lever pro	konfigurierbar/nachrüstbar
MC-Zylinder	nachrüstbar
Remoteleser	standardmässig vorhanden
Kompaktleser	standardmässig vorhanden

Das S-Modul wird mit Hilfe der Systemsoftware konfiguriert.

Einschränkungen sind:

- Die Kombination aus S-Modul Schaltfunktionen, Passlock und Passmode ist nicht möglich.
- Die externe Spannungsversorgung des Geräts ist mit dem S-Modul möglich.
- Die Funktion wird beim Betrieb unter OSS-SO nicht unterstützt.

3.9.4 Wiedereintrittsfunktion (Escape Return) bei c-lever pro

Die Funktion Escape Return gewährleistet für den Notfall (z. B. Feuer) den ungehinderten Wiedereintritt in verlassene Räume ohne Medien.
Denn für den Fall, daß eine Person den Raum ohne Medium verlässt, bleibt der Raum unverschlossen. Der Raum wird beim Verlassen mit dem Medium oder dem Betätigen des Tasters verschlossen.

Einschränkungen sind:

- Die Funktion kann nur mit c-lever pro Komponenten angewendet werden.
- Die Funktion kann mit den Funktionen TimePro und Pass-Lock nicht angewendet werden.
- Die Kombination aus S-Modul Schaltfunktionen und Wiedereintrittsfunktion ist nicht möglich.
- Die externe Spannungsversorgung des Geräts ist mit dem S-Modul möglich.

3.9.5 Pass-Mode bei c-lever pro

Der Pass-Mode ist eine Option für den elektronischen Beschlag c-lever pro. Die Funktion wird mit einem Taster ein- und ausgeschaltet. Durch die Betätigung des Tasters (keine Benutzermedien notwendig) bleibt die Tür offen. Mit dem erneuten Betätigen des Tasters oder durch das Präsentieren eines berechtigten Benutzermediums wird der elektronische Beschlag der Tür wieder in den geschlossenen Zustand versetzt. Der aktuelle Zustand der Tür kann

durch eine kurze Betätigung des Tasters jederzeit abgefragt werden.
Wenn die Hardware erkannt wird, werden vorkonfigurierte Einstellungen geladen.
Der Pass-Mode wird mit Hilfe der Systemsoftware konfiguriert.

Einschränkungen sind:

- Die Kombination aus S-Modul Schaltfunktionen, Passlock und Passmode ist nicht möglich.
- Die externe Spannungsversorgung des Geräts ist mit dem S-Modul möglich.
- Die Funktion wird beim Betrieb unter OSS-SO nicht unterstützt.
- Der Betrieb von Pass-Mode über Wireless wird ab Firmware-Version 42.38 unterstützt.

3.9.6 Pass-Lock bei c-lever pro

Pass-Lock ist eine Option für den elektronischen Beschlag c-lever pro. Die Funktion wird mit dem Taster am Beschlag aktiviert. Wenn der Taster betätigt wird, bleibt die Tür für Personen von außen geschlossen. Durch Präsentieren eines berechtigten Mediums (Master- oder Benutzermedium) wird der c-lever pro wieder in den offenen Zustand versetzt. Von innen kann die Tür immer geöffnet werden.
Pass-Lock wird mithilfe der Systemsoftware konfiguriert. Um eine unbeabsichtigte Aktivierung zu verhindern, kann eine Verzögerung von 0,1 bis 5 Sekunden konfiguriert werden. Pass-Lock wird nur aktiviert, wenn der Taster während der gesamten konfigurierten Verzögerung gedrückt gehalten wird.

Einschränkungen

- Die Kombination aus S-Modul-Schaltfunktionen, Pass-Lock und Pass-Mode ist nicht möglich.
- Die externe Spannungsversorgung des Geräts ist mit dem S-Modul möglich.
- Die Funktion wird beim Betrieb unter OSS-SO nicht unterstützt.
- Der Betrieb von Pass-Lock über Wireless wird ab Firmware-Version 42.38 unterstützt.
- Die Aktivierungsverzögerung ist in der Systemsoftware konfigurierbar. Ist keine Verzögerung explizit konfiguriert, gilt das Standardverhalten (keine Verzögerung). Diese Option ist ab Version 42.48 verfügbar.

3.9.7 Interventionsmedien



Diese Funktion ist ab Firmware-Version 42.48 verfügbar.

Die evolo Komponenten unterstützen ein Zwei-Ebenen-Berechtigungsmodell (2LA). Zusätzlich zur Standardgruppe der berechtigten Benutzer kann einer zweiten, separat definierten Gruppe von Medien eine erweiterte Berechtigung für bestimmte Zutrittssituationen zugewiesen werden. Diese Interventionsgruppe ist unabhängig von der Standardberechtigung und kann auch in Situationen Zutritt erhalten, in denen normale Benutzermedien eingeschränkt oder gesperrt sind, z. B. wenn Pass-Lock aktiv ist oder ein Einbruchdetektionssystem (IDS) scharf gestellt ist. Die folgenden Anwendungsfälle werden unterstützt:

Interventionsmedien für Pass-Lock
Wenn Pass-Lock aktiv ist, wird eine Tür normalerweise nur durch Präsentieren eines Master-Mediums oder eines beliebigen berechtigten Benutzermediums wieder in den offenen Zustand versetzt. Für diesen Zweck kann eine dedizierte Gruppe von Interventionsmedien konfiguriert werden. Im Unterschied zu allen anderen berechtigten Benutzern dürfen dann nur Mitglieder dieser Gruppe Pass-Lock deaktivieren. Dies ist sinnvoll, wenn der Personenkreis, der eine Sperre aufheben darf, eingeschränkt werden soll, z. B. auf bestimmtes Sicherheitspersonal oder Personal des Facility-Managements.

Interventionsmedien für IDS
Wenn ein Einbruchdetektionssystem (IDS) scharf gestellt ist, werden normalerweise alle Medien abgewiesen, bis das IDS unscharf gestellt wird. Es kann eine spezielle Gruppe von Interventionsmedien definiert werden, die auch bei scharf gestelltem IDS Zutritt behält. So können bestimmte Personen, z. B. Einsatzkräfte, unabhängig vom Alarmzustand Zutritt zu den Räumlichkeiten erhalten.

Einschränkungen

- Interventionsmedien für IDS werden nur im Wireless-Betrieb unterstützt und erfordern ein Wireless Gateway 90 40-K7 ab Firmware-Version 5.1.

- Das Scharfstellen des IDS ist eine MATRIX-Funktion. Informationen zur Konfiguration sind in der Dokumentation des Hostsystems MATRIX beschrieben.
- Interventionsmedien werden mit der Systemsoftware konfiguriert. Informationen zur Konfiguration sind im Handbuch der Systemsoftware beschrieben.

3.9.8 Manuelles Programmieren deaktivieren

Bei Verwendung der Systemsoftware und des Programmer 1460 ist das manuelle Programmieren von Komponenten mit Medien deaktiviert.

3.10 TouchGo

Das elektronische Schließsystem TouchGo ist ein Zutrittsberechtigungssystem, das als eine eigenständige Anlage oder eine Komforterweiterung zum dormakaba evolo Subsystem verwendet werden kann. Die Grundlage für diesen Komfort bildet die RCID-Technologie. Siehe Kapitel Sicherheitsaspekte [▶ 3.10.2].

Das TouchGo System ist in zwei unterschiedlichen Varianten verfügbar. Diese definieren den Funktionsumfang der Komponenten. In Kombination mit einem evolo Subsystem werden nur Komponenten der Variante TouchGo E310 verwendet.

Ein TouchGo System ermöglicht es, Türen aufzuschließen, ohne daß ein Schlüssel oder ein Benutzermedium dazu in die Hand genommen werden muss. Nur durch das Berühren der Komponente wird erkannt, ob die Person ein berechtigtes Benutzermedium bei sich trägt. Dafür genügt es, wenn das Benutzermedium auf eine Distanz von ca. 5-10 cm zum Körper getragen wird, wie zum Beispiel in der Hosentasche, in der Jackentasche oder in der Handtasche.

Einschränkungen:

- TouchGo kann mit der Funktion Wireless nicht angewendet werden.

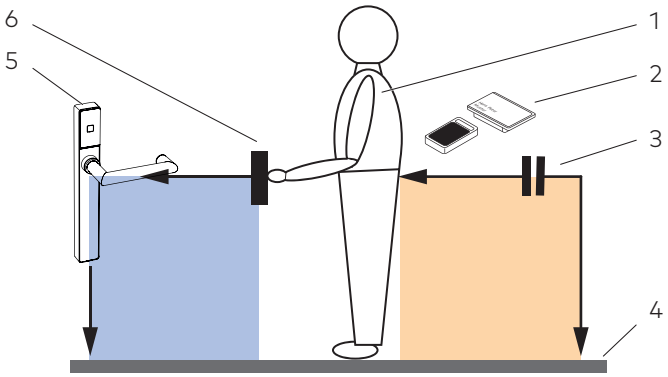
Weiterführende Dokumente

- Planungsrichtlinie dormakaba c-lever pro TouchGo mit S-Modul
- Bedienungsanleitung dormakaba c-lever pro TouchGo

3.10.1 Funktionsweise RCID

RCID: Resisitve Capacitive Identification

Bei Berührung der Komponente (6 zu 5) wird ein in Körpernähe getragenes RCID-Medium (2) identifiziert und die Berechtigung ausgewertet.



1 Person
2 RCID-Medien
3 Kapazitive Signalübertragung (orange)
4 Gemeinsame Masse (Fußboden)
5 TouchGo Komponente
6 Resistive Signalübertragung über den Drücker (blau)

3.10.2 Sicherheitsaspekte

Die RCID-Technologie unterscheidet sich von den herkömmlichen Lösungen dadurch, daß die Informationsübertragung über das elektrostatische Feld des Körpers [▶ 3.10.1] erfolgt, ohne dabei den Komfort und die Sicherheit einzuschränken. Gleichzeitig werden die flexiblen und sicheren Funktionen von elektronischen Schließsystemen beibehalten. Siehe Kapitel Sicherheit mit CardLink-Berechtigungen LEGIC [▶ 5.2] und Kapitel Sicherheit mit der Whitelist-Berechtigung LEGIC [▶ 5.3].

Die Sicherheit des Gesamtsystems ist mit TouchGo jederzeit gewährleistet, denn ein verloren gegangenes Benutzermedium ist einfach und schnell gelöscht. Somit werden gleichzeitig Sicherheitslücken und das kostenintensive Ersetzen ganzer Schließanlagen vermieden.

3.10.3 TouchGo E110

Der TouchGo E110 kann mit den dazugehörenden Medien für maximal 100 Benutzer verwendet werden. Er besitzt die TouchGo Office Mode Funktion. Der TouchGo E110 kommt vollständig ohne Programmiergeräte und Systemsoftware aus.



Der TouchGo E110 ist standalone und kann nicht in einem evolo-Subsystem verwendet werden.

Die Programmierung des TouchGo E110 ist in der Bedienungsanleitung zum c-lever pro TouchGo beschrieben.

3.10.4 TouchGo E310

Die TouchGo E310 Komponenten lassen sich einfach in die gewählte Systemsoftware einbinden, ohne an Sicherheit zu verlieren. Das TouchGo E310 ist eine Komfortoption, die keinen Einfluss auf ein Sicherheitsdispositiv hat.

Im evolo Subsystem wird zur eindeutigen Identifizierung und Verwaltung auf die bewährte RFID-Technologie zurückgegriffen. Dazu werden die RFID-Daten in der Komponente beim Auslesen mit den Daten der TouchGo-Technologie „verheiratet" (Pairing). Das bedeutet, dass die vergebene Zutrittsberechtigung auf TouchGo übertragen wird und die Komponente diese über Berührung erkennt.

Zukünftige Änderungen in der Berechtigung, übertragen durch den Programmer (Whitelist-Berechtigung) oder die RFID-Technologie (CardLink-Berechtigung), werden automatisch auch in TouchGo übernommen. Bei Verlust oder Ausfall des Kombimediums oder ausschließlich des Pairing Partners kann die Berechtigung umgehend gelöscht werden. Im anderen Fall können die einzelnen Komponenten weiterhin verwendet werden, denn ein erneutes „Verheiraten" kann jederzeit direkt an den Komponenten vorgenommen werden.



TouchGo kann mit der Funktion Wireless nicht angewendet werden.

3.10.4.1 Whitelist-Berechtigung mit TouchGo

Bei Schließanlagen mit Whitelist-Berechtigung kann der zusätzliche Komfort von TouchGo für die TouchGo Komponenten genutzt werden. Das TouchGo RFID/RCID-Kombimedium wird, wie das RFID-Medium, einfach mit RFID-Programmiermedien in die Komponente programmiert oder auf den Tischleser gelegt und die Daten der RFID-Technologie in der Systemsoftware registriert. Die Zutrittsberechtigung der RFID-Technologie wird mit dem Programmer an die Komponenten verteilt. Das Kombimedium wird der standalone Komponente präsentiert und beim Auslesen der RFID-Daten mit der TouchGo-Technologie „verheiratet" (Pairing). Die gleiche Zutrittsberechtigung wird zu TouchGo übertragen und die Komponente erkennt die Berechtigung über eine Berührung.

Zukünftige Änderungen in der Berechtigung werden automatisch auch in TouchGo übernommen.

3.10.4.2 CardLink-Berechtigung mit TouchGo

Auch bei Schließanlagen mit CardLink-Berechtigungen kann der zusätzliche Komfort von TouchGo für die TouchGo Komponenten genutzt werden. Die Berechtigungsvergabe findet in der Systemsoftware statt und wird über die RFID-Technologie an die standalone Komponenten übertragen.

Gleichzeitig zur Übertragung wird TouchGo "verheiratet" (Pairing). Das bedeutet, dass die vergebene Zutrittsberechtigung auf TouchGo übertragen wird und die Komponente diese über eine Berührung erkennt.

Zukünftige Änderungen in der Berechtigung und die Erneuerung der Validierung werden über die RFID-Technologie an die standalone Komponenten übertragen und gleichzeitig wird das "Verheiraten" (Pairing) geprüft.

3.11 Freie Schrankwahl beim Schrankschloss 21 10 und 21 20

Diese Option ist nur bei den Schrankschloss-Modellen 21 10 und 21 20 verfügbar.

Im Zutrittsmodus CardLink oder Whitelist wird die Berechtigung für einen Schrank dem Benutzer wie bei einer normalen Komponente zugewiesen. Im Zutrittsmodus „Freie Schrankwahl mit CardLink" oder „Freie Schrankwahl mit Whitelist" können die Benutzer selbst einen freien Schrank belegen, für den sie berechtigt sind. Ein Zutrittsmodus muss konfiguriert sein. Die Anzahl der belegbaren Schränke für den einzelnen Benutzer wird mithilfe des Schrankschloss-Assistenten auf dem Benutzermedium festgelegt. Es können ein bis vier Schränke belegt werden. Ein belegter Schrank kann nur mit dem entsprechenden Benutzermedium oder mit einem Servicemedium geöffnet werden. Dabei wird die Benutzerauswahl gelöscht und der Schrank ist wieder frei.

Schrankbelegungen können mit den Verwaltungstools des Hostsystems gelöscht werden, beispielsweise mit dem Schrankschloss-Assistenten im dormakaba evolo Manager (KEM).

3.12 Briefkasten/Aufzug

Ein Benutzer kann mit dem Benutzermedium nur die Briefkästen öffnen oder im Aufzug nur die Stockwerke anfahren, für die er auch die Berechtigung besitzt.

Briefkasten/Aufzug kann nur über die Systemsoftware konfiguriert werden.
Mobile Access ist möglich ab FW 42.38
Wireless ist nicht möglich.

Eine Einheit besteht aus einem Remoteleser 91 15 und bis zu 6 Modulen 90 30 mit je 8 geschalteten Ausgängen. Die Anzahl der Module ist abhängig von der Anzahl der benötigten Ausgänge. Maximal 49 Ausgänge können so konfiguriert werden.

Verhältnis Ausgänge zu benötigte Komponenten:

Anzahl Ausgänge	Anzahl Komponenten
1	91 15 (Remoteleser mit 1 Relaisausgang)
bis 9	91 15 + 1 x 90 30 (Erweiterungsmodul mit 8 Relaisausgängen)
bis 17	91 15 + 2 x 90 30
bis 25	91 15 + 3 x 90 30
bis 33	91 15 + 4 x 90 30
bis 41	91 15 + 5 x 90 30
bis 49	91 15 + 6 x 90 30

4 Systemvarianten

Das evolo Subsystem kann in verschiedenen Systemvarianten eingesetzt werden und bleibt in allen Varianten ausbaufähig.

Die gewählten Beispiele sind mit LEGIC und mit MIFARE Medien durchführbar, auch wenn im Bild überwiegend LEGIC dargestellt ist. Der Unterschied besteht in den verwendeten Sicherheitskarten. Bei LEGIC werden die Sicherheitskarten C1 und C2 verwendet, bei MIFARE die Sicherheitskarte C.

4.1 Whitelist Programmierung

4.1.1 Whitelist-Berechtigung ohne Toolkette

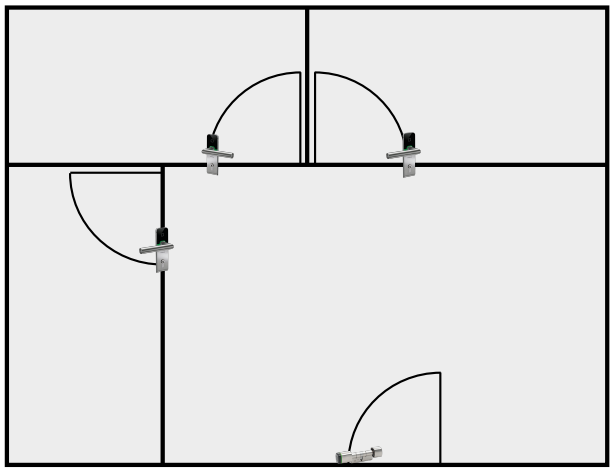
Bei kleinen Schließanlagen werden die Benutzermedien direkt mit einem Master in die Komponenten einprogrammiert. Für diese Methode wird keine Systemsoftware und kein Programmer benötigt. Wireless oder Mobile Access sind ebenfalls nicht möglich.

Die Programmierung ist im Kapitel Programmieren mit Medien beschrieben.

Master A, Master B und Benutzermedien



Anlagenbeispiel:

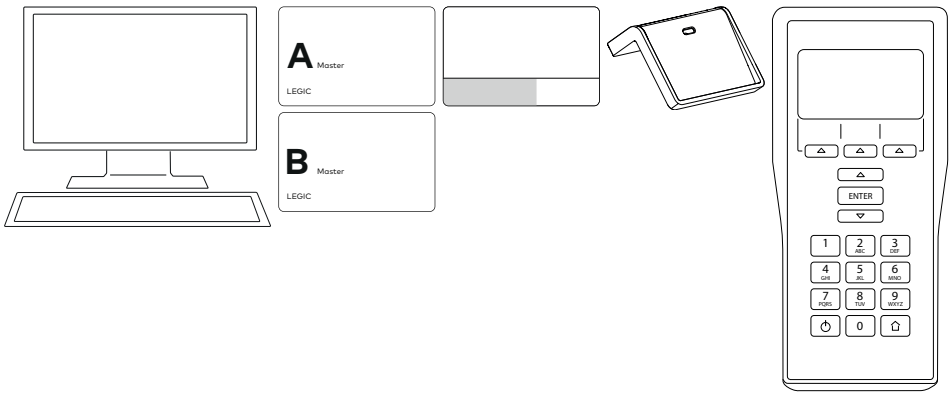


4.1.2 Whitelist-Berechtigung mit Toolkette

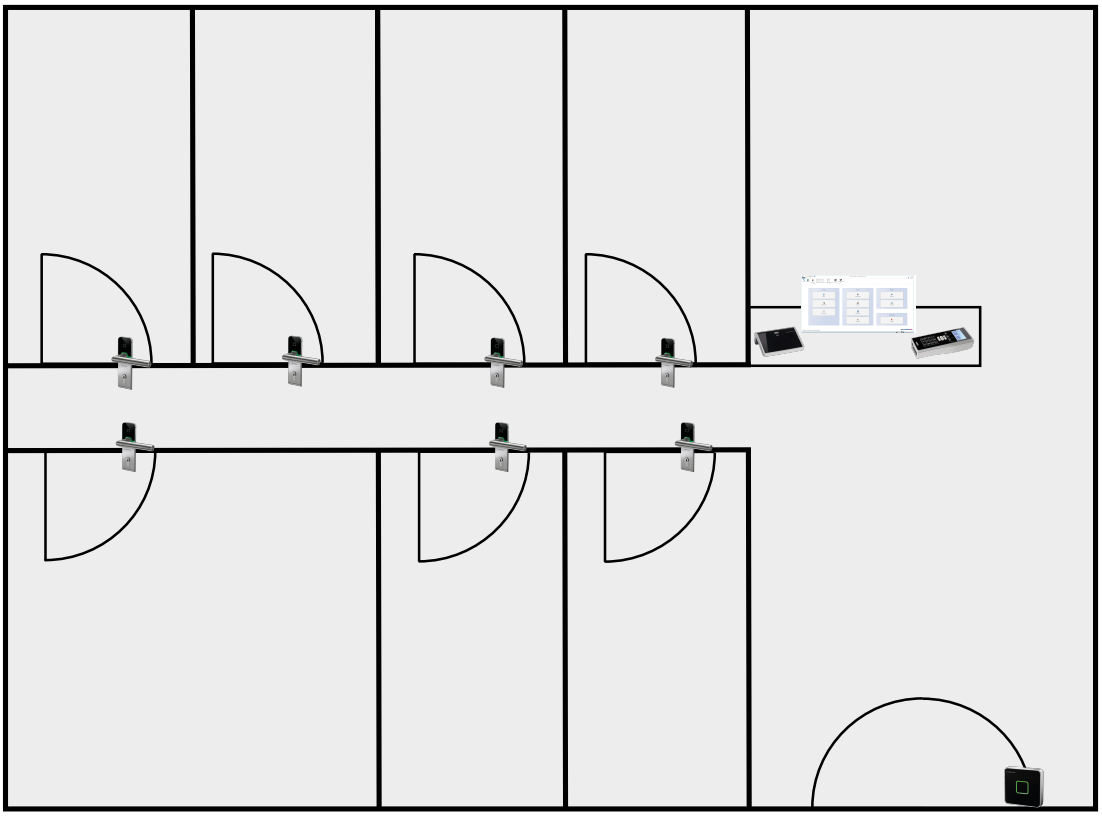
Bei größeren Schließanlagen mit Zeitmanagement werden die Benutzermedien mit der Systemsoftware verwaltet. Die Berechtigungsdaten werden mit dem Programmer von der Software in die Komponenten übertragen oder über Wireless aktualisiert. Im Beispiel ohne Wireless.

Die Programmierung ist im Kapitel Programmieren mit Systemsoftware und Programmer [▶ 7.5.2] beschrieben.

Toolkette: Systemsoftware mit Master, Benutzermedien, Tischleser und Programmer



Anlagenbeispiel:



4.2 CardLink Programmierung

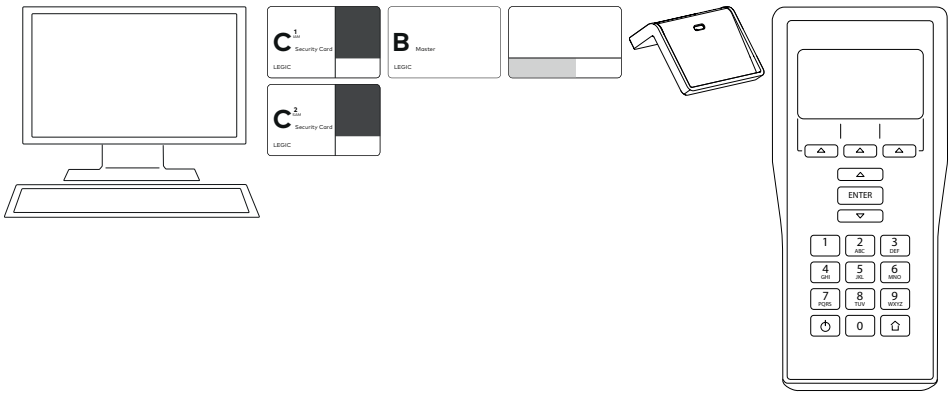
CardLink wird mithilfe der Systemsoftware programmiert.

Die Programmierung ist im Kapitel Programmieren mit Systemsoftware beschrieben

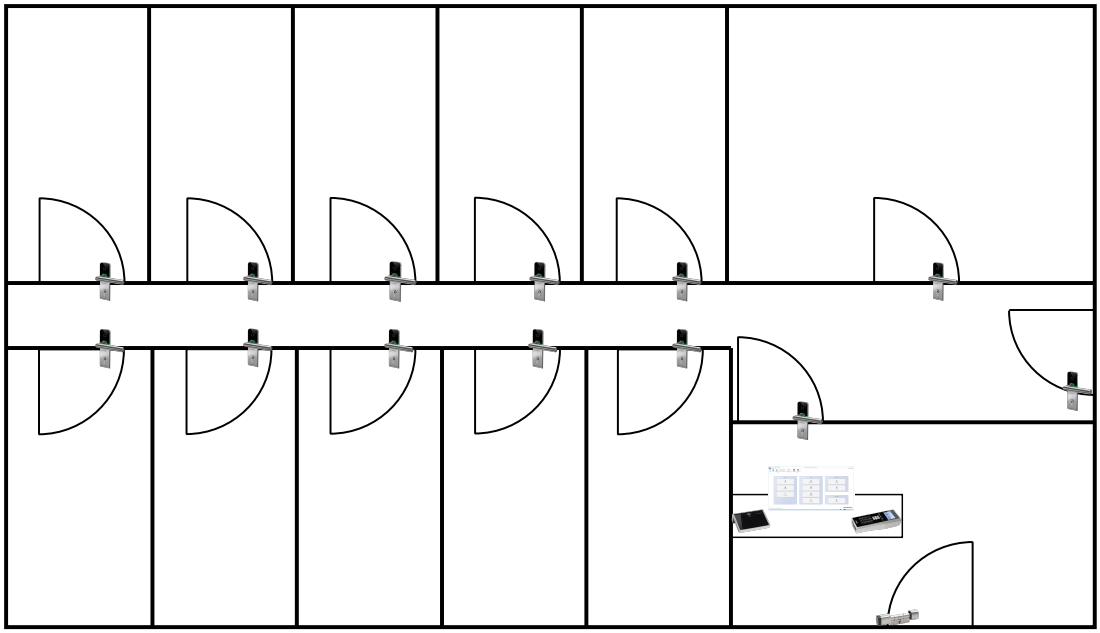
4.2.1 CardLink-Berechtigung über Tischleser

Bei CardLink Schließanlagen werden die Benutzermedien mit der Systemsoftware organisiert. Die Berechtigungen werden mit dem Tischleser in die Benutzermedien geschrieben. Die Komponenten benötigen nur eine Initialisierung für Cardlink. Neue Berechtigungen werden von der Systemsoftware mit dem Tischleser in die Benutzermedien übertragen. Die Validierungen übernehmen in dem Fall die einzelnen standalone Komponenten, die hierfür konfiguriert wurden. Die Wireless-Funktion wird ebenfalls unterstützt.

Toolkette: Systemsoftware mit Sicherheitskarte, Master, Benutzermedien, Tischleser und Programmer



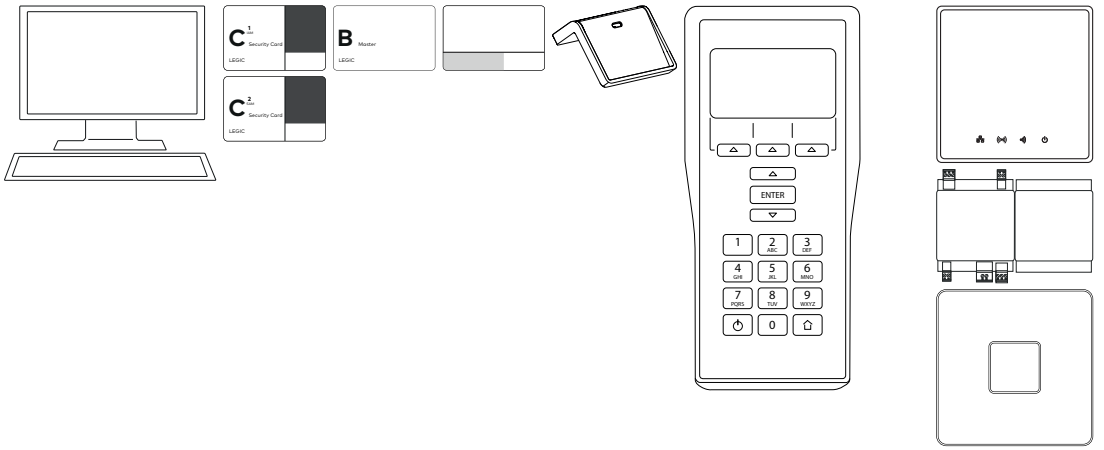
Anlagenbeispiel:

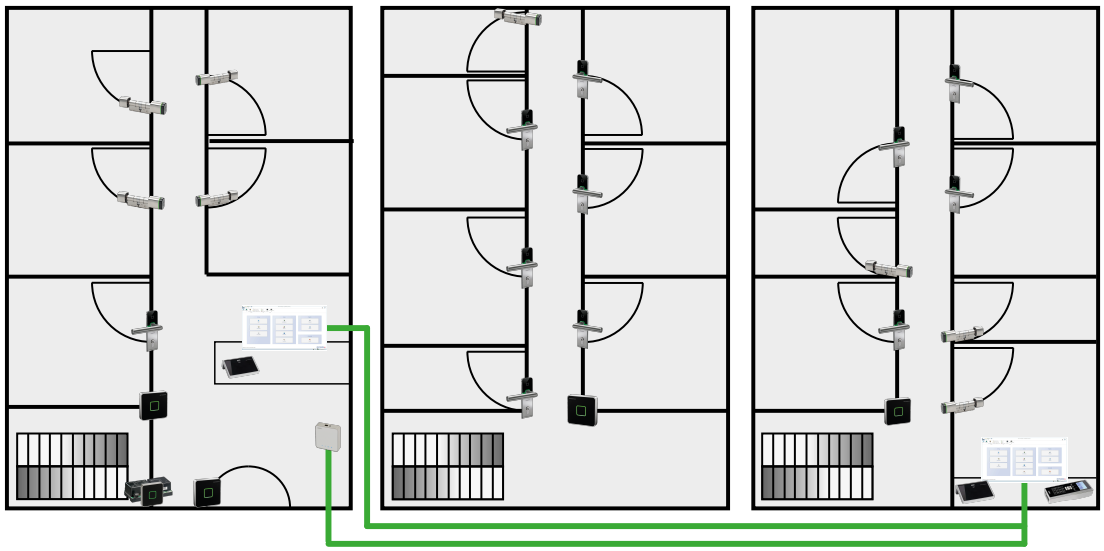


4.2.2 CardLink-Berechtigung über Update Reader

Für die Vergabe neuer Zutrittsberechtigungen in die Benutzermedien wird anstelle des Terminals ein Cardlink Update Reader eingesetzt. Der Reader ist über ein wireless Gateway* mit der Systemsoftware verbunden. Damit lassen sich neue Zutrittsberechtigungen für die Benutzer zeitunabhängig online erteilen oder entziehen. Die Validierungen übernimmt in dem Fall der update Reader.

Toolkette: Systemsoftware mit Sicherheitskarte, Master, Benutzermedien, Tischleser, Programmer, Gateway und update Reader 91 15 mit Erweiterungsmodul 90 43.





CardLink-Berechtigungen ohne wireless Gateway auf Update Reader übertragen

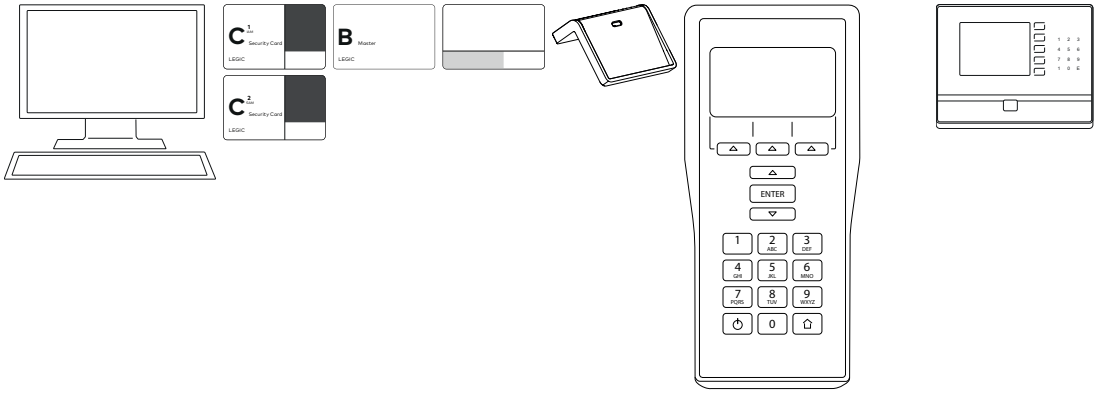
Die CardLink-Berechtigungen können mit dem Programmer 1460 auf den Update Reader übertragen werden.

Der Komfort der online und zeitunabhängig erteilten Zutrittsberechtigungen entfällt daduch.

4.2.3 CardLink-Berechtigung über Terminal

Diese Art von CardLink-Berechtigung eignet sich besonders für Schließanlagen mit immer wiederkehrenden Veränderungen der Benutzerberechtigungen. Für das Vergeben von neuen Zutrittsberechtigungen in die Benutzermedien wird das Terminal eingesetzt, das mit der Systemsoftware verbunden ist. Damit lassen sich neue Zutrittsberechtigungen für die Benutzer zeitunabhängig erteilen oder entziehen. Die Validierungen übernimmt in dem Fall das Terminal.

Toolkette: Systemsoftware mit Sicherheitskarte, Master, Benutzermedien, Tischleser, Programmer und Terminal



Anlagenbeispiel:



4.3 Übersicht Firmware-Varianten

Funktion / Firmware	E300[A]	E305[B]	E310[C]	E320[D]	E321[E]	E340[F]	E360[G]	E361[H]
Master A	1	1	1	1	1	1	1	1
Master B	bis zu 200	bis zu 200	bis zu 200	bis zu 200	bis zu 200	bis zu 200	bis zu 200	bis zu 200
Whitelist-Berechtigungen								
Whitelist-Einträge (UID/ Card ID) – Offline-Modus	4000	1000	1000[5]	4000	4000 (Offline-Modus)	4000	4000 (Offline-Modus)	4000 (Offline-Modus) bis zu 30.000 (Online-Betrieb mit Gateway 9040-K7)
Whitelist-Einträge (UID/ Card ID) – Online-Modus mit Wireless Gateway 9040-K7				bis zu 30.000	bis zu 30.000		bis zu 30.000	bis zu 30.000
Zeitabhängige Berechtigungen	✓	✓	✓	✓	✓	✓	✓	✓
Manuelles Programmieren deaktivieren	✓	✓	✓	✓	✓	✓	✓	✓
CardLink-Berechtigungen								
Validierung	✓	—	✓	✓	✓	✓	✓	✓
Einzelrecht Tür[4]	bis zu 60	—	bis zu 60	bis zu 60	bis zu 60	bis zu 60	bis zu 60	bis zu 60
Einzelrecht Türgruppe[4]	bis zu 39	—	bis zu 39	bis zu 39	bis zu 39	bis zu 39	bis zu 39	bis zu 39
Reservation Einzelrecht Tür[4]	bis zu 18	—	bis zu 18	bis zu 18	bis zu 18	bis zu 18	bis zu 18	bis zu 18
Reservation Einzelrecht Türgruppe[4]	bis zu 11	—	bis zu 11	bis zu 11	bis zu 11	bis zu 11	bis zu 11	bis zu 11
Türgruppen-Recht	512	—	512	512	512	512	512	512
Blacklist-Einträge	400	—	400	400	400	400	400	400
Servicemedien	✓	—	✓	✓	✓	✓	✓	✓
Medien-Traceback[3]	60	—	60	60	60	60	60	60
TouchGo Medien	—	—	1000	—	—	—	—	—
Erweiterte Funktionen								
Wireless	—	—	—	✓	✓	—	✓	✓
Komponenten-Traceback-Speicher	2000	2000	2000	2000	2000	2000	2000	2000
Pass-Mode[1]	Option	—	Option	Option	Option	Option	Option	Option

Funktion / Firmware	E300[A]	E305[B]	E310[C]	E320[D]	E321[E]	E340[F]	E360[G]	E361[H]
Zeitprofile	15 und „Immer"	15 und „Immer"	15 und „Immer"	15 und „Immer"	15 und „Immer"	15 und „Immer"	15 und „Immer"	15 und „Immer"
Zeitfenster für jedes Zeitprofil	12	12	12	12	12	12	12	12
Ferienperioden	20	20	20	20	20	20	20	20
Sondertage A+B	32+32	32+32	32+32	32+32	32+32	32+32	32+32	32+32
TimePro-Funktionen	✓	✓	✓	✓	✓	✓	✓	✓
S-Modul[2]	Option	—	Option	Option	Option	Option	Option	Option
Master T und Servicemedium	✓	✓	✓	✓	✓	✓	✓	✓
Mobile Access								
NFC/HCE	✓	—	—	✓	✓	✓	✓	✓
Bluetooth	—	—	—	—	—	✓	✓	✓

Legende:

1 Nur für c-lever pro.

2 Standard für Leser, optional für c-lever pro.

3 Nur mit MIFARE DESFire und LEGIC advant Medien.
Abhängig von der Segment-/Dateigröße
Standardwert gemäß Medienspezifikation. Kann größer oder kleiner sein.

4 Je nach den verwendeten Berechtigungsarten.

5 RCID und RFID.

A E300 – evolo V4

B E305 – Briefkasten/Aufzug
E345 – Briefkasten/Aufzug mit Mobile Access

C E310 – TouchGo

D E320 – Wireless

E E321 – Wireless mit Türüberwachung
Zusätzliche Komponenten wie Türrahmenkontakte und Schlosssensoren (Falle, Riegel) sind erforderlich.

F E340 – Mobile Access

G E360 – Wireless und Mobile Access

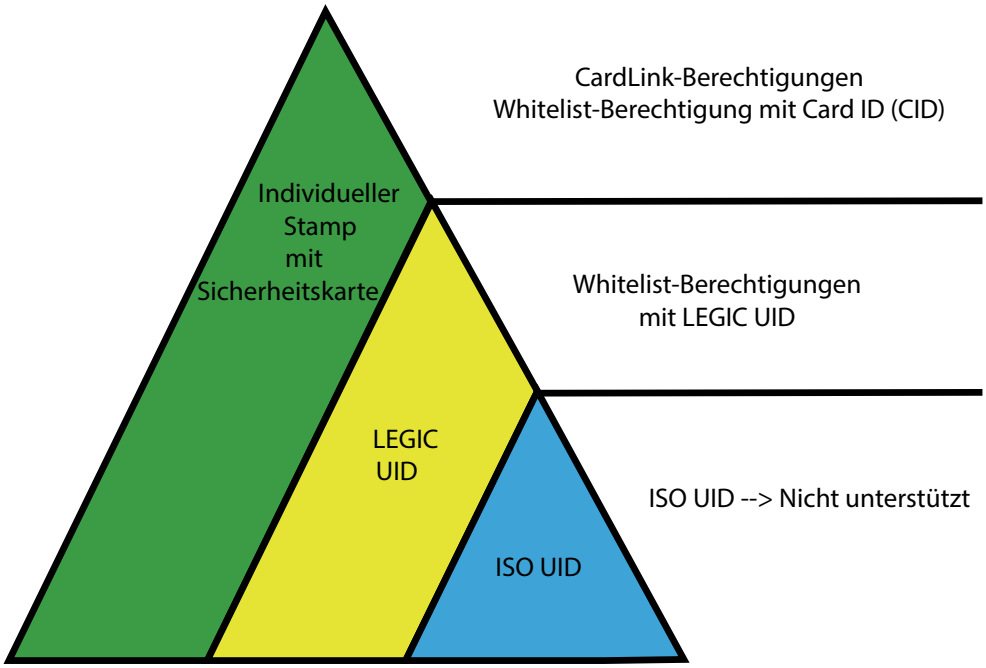
H E361 – Wireless mit Türüberwachung und Mobile Access
Zusätzliche Komponenten wie Türrahmenkontakte und Schlosssensoren (Falle, Riegel) sind erforderlich.

5 Sicherheitsfunktionen

Das Kapitel beschreibt die möglichen Sicherheitsfunktionen für LEGIC und MIFARE in Schließanlagen, die nach den gewünschten Sicherheitsanforderungen ausgewählt werden können.

5.1 Die Sicherheitsstufen LEGIC

Für die Berechtigungsarten stehen folgende Sicherheitsstufen zur Auswahl.



Individueller Stamp
Für jede Schließanlage wird ein individueller Stamp definiert. Dieser Stamp dient zur Identifikation der anlagenspezifischen LEGIC-Medien. Der Stamp wird durch die Sicherheitskarte C1 oder C2 in der jeweiligen Schließanlage definiert.

LEGIC UID
Die LEGIC UID wird für normale Schließanlagen mit Whitelist eingesetzt. Bei LEGIC UID wird die Unikatsnummer (UID) zusätzlich über eine LEGIC-Funktion auf den Medien verifiziert.

Hinweis: Die Systemsoftware KEM verwendet ausschließlich die LEGIC UID.

5.2 Sicherheit mit CardLink-Berechtigungen LEGIC

Individueller Stamp
Mit dem Einsatz einer CardLink-Berechtigung wird mit LEGIC ein individueller Stamp notwendig.

Jede elektronische Komponente sowie der Tischleser verfügen über LEGIC-Hardware, die mit diesem Stamp arbeiten. Damit der anlagenspezifische Stamp in die Schließanlage integriert werden kann, wird die Sicherheitskarte C1 und/oder C2 benötigt. Mit dieser Sicherheitskarte wird der Stamp an die jeweilige Komponente übertragen. Für jede Schließanlage wird eine neue Sicherheitskarte benötigt. Wenn ein Stamp verwendet wird, sind die Systemsoftware KEM, der Tischleser und die jeweiligen Komponenten damit zu initialisieren. Anschließend muss die Sicherheitskarte an einem sicheren Ort (z.B. Tresor) aufbewahrt werden.

5.3 Sicherheit mit der Whitelist-Berechtigung LEGIC

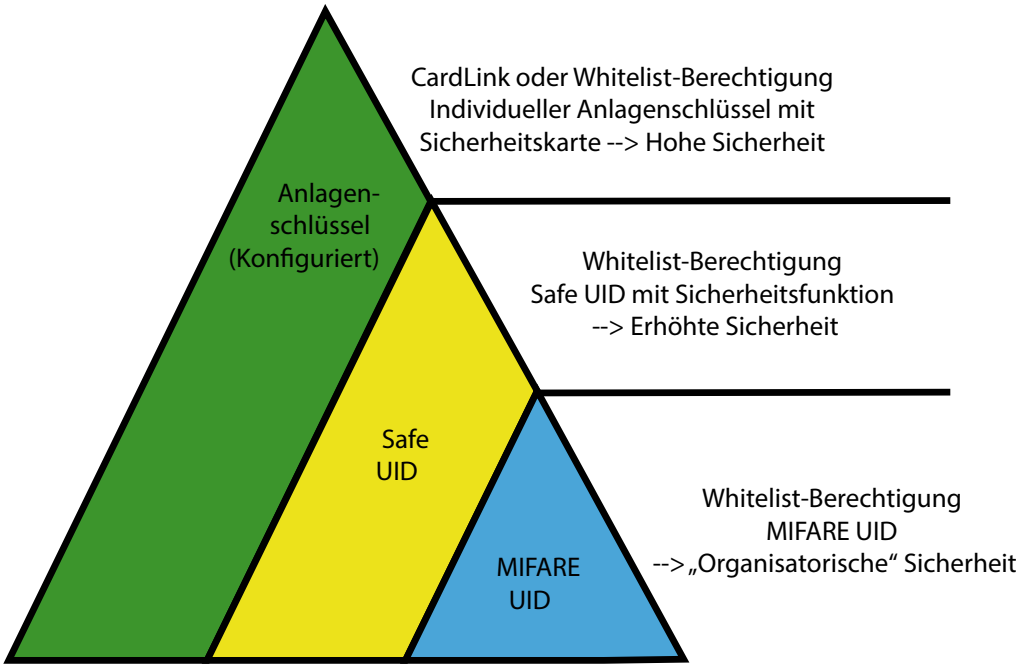
Card ID (CID)
Anstelle der UID wird den Medien eine individuelle CID vom System vergeben.

Diese CID wird mit einem individuellen LEGIC-Stamp in den Medienspeicher geschrieben. Definiert wird dieser Stamp durch die Sicherheitskarte C1. Für jede Anlage wird eine eigene Sicherheitskarte benötigt, um die Sicherheit zu gewährleisten. Wird der individuelle LEGIC-Stamp verwendet, sind die Systemsoftware KEM und der Tischleser damit zu initialisieren. Anschließend muss die Sicherheitskarte an einem sicheren Ort (z. B. Tresor) aufbewahrt werden.

LEGIC UID
Bei LEGIC UID wird die LEGIC-Funktion zur Sicherung der UID (Unikatsnummer) der Benutzermedien genutzt. Die Sicherheit einer UID wird dadurch bedeutend verbessert, da die LEGIC-Funktion die UID verifiziert.

5.4 Die Sicherheitsstufen MIFARE

Für die Berechtigungsarten stehen folgende Sicherheitsstufen zur Auswahl.



Anlagenschlüssel (Sitekey)
Der Anlagenschlüssel eignet sich für den Einsatz in Schließanlagen mit hohen Sicherheitsansprüchen.

Der Anlagenschlüssel ist ein spezifischer Schlüssel, der individuell jeder einzelnen Schließanlage zugewiesen wird. Dieser Schlüssel wird von einem Sicherheitschip automatisch erzeugt. Dieser zusätzliche Sicherheitschip ist in jeder Komponente integriert und regelt nach der Initialisierung das individuelle Ver- und Entschlüsseln aller Daten, die vom System in die Benutzermedien geschrieben werden.

Safe UID
Diese Sicherheitsstufe wird für normale Schließanlagen eingesetzt.

Bei Safe UID wird die Unikatsnummer (UID) zusätzlich verschlüsselt auf dem Medienspeicher abgelegt. Die UID wird nur dann als gültig erkannt, wenn die Daten in den Benutzermedien übereinstimmen.

MIFARE UID
Diese Sicherheitsstufe eignet sich primär für organisatorische Anwendungen.

MIFARE Medien entsprechen dem ISO Standard 14443A. Darin wird definiert, dass die Unikatsnummer (UID) ohne weiteren Schlüssel ausgelesen werden kann. In dieser Sicherheitsstufe wird ausschließlich die UID des Transponders zur Identifikation benutzt.

5.5 Sicherheit mit CardLink Berechtigungen MIFARE

Anlagenschlüssel
Mit dem Einsatz einer CardLink Berechtigung oder eines Master T wird ein Anlagenschlüssel (Sitekey) notwendig.

Jede elektronische Komponente sowie der Tischleser verfügen über die spezielle Sicherheitshardware, die mit diesem Anlagenschlüssel arbeiten. Damit der spezifische Schlüssel in die Schließanlage integriert werden kann, wird die Sicherheitskarte C der betreffenden Anlage benötigt. Mit dieser Sicherheitskarte wird der Anlagenschlüssel an die jeweilige Schließanlage übertragen. Für jede Schließanlage wird eine individuelle Sicherheitskarte benötigt.

Wenn ein Anlagenschlüssel verwendet wird, sind die Systemsoftware, der Tischleser und die jeweiligen Programmiermedien damit zu initialisieren. Anschließend muss die Sicherheitskarte an einem sicheren Ort (z. B. Tresor) aufbewahrt werden.

5.6 Sicherheit mit der Whitelist Berechtigung MIFARE

Card ID (CID)
Statt der UID wird den Medien eine individuelle CID vom System vergeben. Diese CID wird mit einem individuellen Anlagenschlüssel verschlüsselt und in den Medienspeicher geschrieben. Dieser Anlagenschlüssel wird durch eine Sicherheitskarte C definiert.

Die Sicherheitskarte C kann über den Vertriebsweg bezogen werden. Mit dieser Sicherheitskarte werden die elektronischen Komponenten mit dem individuellen Schlüssel der Anlage initialisiert. Für jede Anlage wird eine individuelle Sicherheitskarte benötigt.

Wenn ein Anlagenschlüssel verwendet wird, sind die Systemsoftware, der Tischleser und die jeweiligen Programmiermedien damit zu initialisieren. Anschließend muss die Sicherheitskarte an einem sicheren Ort (z. B. Tresor) aufbewahrt werden.

Safe UID
Die Sicherheitsstufe Safe UID eignet sich für Anwendungen mit erhöhten Sicherheitsansprüchen.

Voraussetzung für den Einsatz der Safe UID ist die Kaba Applikation KCA in den Benutzermedien. Bei der Safe UID wird die UID (Unikatsnummer) der Medien zusätzlich durch eine spezielle Applikation in den Medienspeichern überprüft. Die Sicherheit einer UID wird dadurch bedeutend verbessert, da der Inhalt der Applikation nicht frei zugänglich und verschlüsselt ist.

MIFARE UID (nach ISO 14443A)
In der Whitelist kann mit der UID (Unikatsnummer) eine Berechtigung programmiert werden.

Wenn die UID dem Standard ISO 14443A entspricht, kann diese in die Whitelist eingetragen werden. Gemäss dem ISO Standard ist diese UID frei auslesbar und nicht weiter gesichert. Der Einsatz dieser Sicherheitsstufe ist nur für organisatorische Anwendungen mit einem niedrigen Sicherheitsanspruch zu empfehlen.

5.7 Master T

Der Master T ist eine Spezialform der Master-Medien für Standalone-Komponenten. In einer Schließanlage verwendete Master T sind nur für eine gewisse Zeit gültig und haben eingeschränkte Funktionen. Damit wird eine hohe Flexibilität in der Verwaltung von Schließanlagen möglich, weil ein Master T an Servicepersonal ausgegeben werden kann, ohne dafür den sicherheitsrelevanten Master A oder B herausgeben zu müssen.



Ein Master T kann nur eingesetzt werden, wenn die Komponenten vorher mit einem Master B und dem Programmer 1460 konfiguriert wurden.

Master T für LEGIC:
Mit der Systemsoftware können Master T Medien für LEGIC definiert werden. Ein Master T wird von der Sicherheitskarte abgeleitet und kann nur als Master T eingesetzt werden.

Master T für MIFARE:
Mit der Systemsoftware können Master T Medien für MIFARE definiert werden. Ein Master T kann von der Sicherheitskarte C abgeleitet werden.

Die Master T Medien für LEGIC und MIFARE besitzen folgende Eigenschaften:

- Anwendung in beiden Berechtigungsarten: CardLink und Whitelist.
- Aktualisierung der Komponenten (die Komponenten müssen konfiguriert sein).
- Einstellen der Uhr der Komponenten.
- Auslesen des Traceback.
- Zeitlich begrenzte Gültigkeitsdauer.

6 Komponenten

Die evolo Komponenten bieten eine Vielzahl von verschiedenen Funktionen, die in der nachfolgenden Übersicht zusammengefasst sind. Für sicherheitsrelevante Bereiche stehen Komponenten mit mechanisch verstärktem Schutz zur Verfügung. Detaillierte Angaben sind in den separaten Bedienungsanleitungen und im Produktkatalog zu finden.

6.1 Speichergrössen

Die folgenden Speichergrössen stehen für den wiederbeschreibbaren Speicher der Benutzermedien zur Verfügung:

	MIFARE		LEGIC
Berechtigungen	**classic**	**DESFire**	**advant**
	in Byte	in Byte	in Byte
Speichergrösse der Benutzermedien	1 k	8 k	4 k
CTC Benutzermedien	—		3 k
Speichergrösse der Standard Applikationen	288	744	848
Kaba Common Application (KCA) Safe UID	48	32	—
CardLink (192 Byte Nutzdaten)	216	192	216
Maximale Anzahl an Berechtigungen auf einem Benutzermedium:			
Maximal 512 Türgruppen konfiguriert:	– bis zu 39 Einzelrechte – bis zu 11 Reservationen		
Ohne Türgruppen:	– bis zu 60 Einzelrechte – bis zu 18 Reservationen		
Statuseinträge:			
Status Komponenten (32 Byte Nutzdaten)	48	32	56
Identifikation (32 Byte Nutzdaten)	48	32	64
Traceback (60 Einträge)	—	488	512

6.2 Technische Daten

Benutzermedien
Karten

Bezeichnung	**Werte**
Farben (Drucklayout)	• dormakaba (rot oder blau) • Ihr individuelles Design
Umgebungsbedingungen	
Schutzart	IP66 Verträgt Nässe, ist aber nicht für das Eintauchen in Wasser geeignet. Die Verwendung als Badeschlüssel wird beispielsweise nicht empfohlen.
Temperatur	-25 ... +70 °C
Luftfeuchtigkeit	0 ... 95% rH, nicht kondensierend
Speicherkapazität der Medien	

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	1 kB/3 kB (LEGIC prime/advant)



Die Karten sind gegen Hacking und Klonen geschützt.

Schlüsselanhänger

Bezeichnung	**Werte**
Farben	Blau, Schwarz, Rot, Weiß
Umgebungsbedingungen	
Schutzart	IP65
Temperatur	-20 ... +55 °C
Luftfeuchtigkeit	0 ... 95% rH, nicht kondensierend
Speicherkapazität der Medien	
A-BE-MID	8 kB (MIFARE DESFire EV3)
A-BE-ADT	4 kB/3,5 kB (LEGIC advant/MIFARE DESFire EV3)
A-BE-CTC	1 kB/3 kB (LEGIC prime/advant)

Schlüssel mit Clip

Bezeichnung	**Werte**
Clip	
Farben	
Clip-Farbeinsätze	Schwarz, Silber, Violett, Gelb, Grün, Rot, Blau
Umgebungsbedingungen	
Schutzart	IP67 Verträgt zeitweiliges Eintauchen in Wasser.
Temperatur	-20 ... +70 °C
Luftfeuchtigkeit	0 ... 95% rH, nicht kondensierend
Speicherkapazität der Medien	
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	1 kB/3 kB (LEGIC prime/advant)
Schlüssel	
Mechanische Schließsysteme	
dormakaba eco	
dormakaba expert	
dormakaba gemini	
dormakaba matrix	
dormakaba penta	
dormakaba quattro	
dormakaba pextra	
dormakaba AP2000	

Kaba star
Kaba star cross
Kaba 20

TouchGo Benutzermedien
Schlüsselanhänger

Bezeichnung	**Werte**
Farben	
Benutzermedien	Schwarz, Weiß
Abmessungen	
B x H x T	36 x 60 x 12 mm
Energieversorgung	
Batterie	3V CR2450 Lithium
Umgebungsbedingungen	
Schutzart	IP 53
Temperatur	-25 ... +65 °C
Luftfeuchtigkeit	0 ... 95% rH, nicht kondensierend
Speicherkapazität der Medien	
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	1 kB/3 kB (LEGIC prime/advant)

Armband

Bezeichnung	**Werte**
Farben	Grau
Abmessungen	
B x H x T	56 x 53 x 17 mm
Energieversorgung	
Batterie	3V CR2450 Lithium
Umgebungsbedingungen	
Schutzart	IP67 (wasserdicht)
Temperatur	-25 ... +65 °C
Luftfeuchtigkeit	0 ... 95% rH, nicht kondensierend
Speicherkapazität der Medien	
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	1 kB/3 kB (LEGIC prime/advant)

Kartenhalter

Bezeichnung	**Werte**
Farben	
Kartenhalter	Schwarz, Silber-Schwarz
Abmessungen	

B x H x T	90 x 58 x 14 mm
Energieversorgung	
Batterie	3V CR2430 Lithium
Umgebungsbedingungen	
Schutzart	IP 53
Temperatur	-25 ... +65 °C
Luftfeuchtigkeit	0 ... 95% rH, nicht kondensierend
Speicherkapazität der Medien	
H-BE-TGO	abhängig vom eingelegten Medium.

6.3 Master-Medien

Mit 2 verschiedenen Typen von Master-Medien, Master A und Master B, können die Komponenten in den Programmier-Modus gesetzt werden (Programmierarten). Diese Medien werden ausschließlich zur Erteilung der Berechtigung eingesetzt und besitzen selbst keine Zutrittsberechtigung.

Master-Medien	MIFARE	LEGIC	Funktionen
Master A 	✓	✓	– Master einer Anlage mit Master A/B-Struktur – Komponenten werden mit Master B in den Programmier-Modus versetzt – Komponenten mit Master B programmieren
Master B 	✓	✓	– Master einer Anlage – Komponenten werden in den Programmier-Modus versetzt – Komponenten mit Benutzermedien programmieren
Master T 	✓	✓	– Master T für das Aktualisieren von Komponenten – nur beschränkte Zeit gültig – eingeschränkte Funktionen
RCID-Master B 			RCID Nur TouchGo E110 – Master einer Anlage – Komponenten werden in den Programmier-Modus versetzt – Komponenten mit Benutzermedien programmieren

6.4 Sicherheitskarten

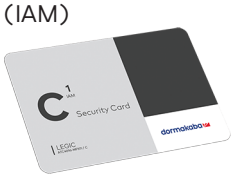
Die Sicherheitskarten werden in einer LEGIC oder in einer MIFARE Umgebung eingesetzt. Je nach verwendeter Technologie unterscheiden sich die Funktionen der Sicherheitskarten.

Für LEGIC gibt es verschiedene Sicherheitskarten:

- Sicherheitskarte C1 für die anlagenspezifische Segmentierung der Medien
- Sicherheitskarte C2 für das Initialisieren der Anlage mit Tischleser und Validierungs-Komponenten in CardLink

Für MIFARE gibt es die Sicherheitskarte C:

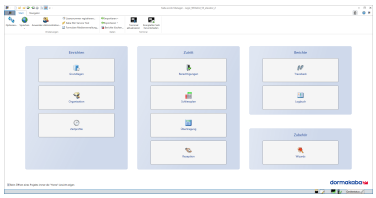
Damit der anlagenspezifische Schlüssel einer MIFARE Umgebung in die Schließanlage integriert werden kann, wird die Sicherheitskarte C benötigt. Diese definiert den Anlagenschlüssel sowie die Speicherorganisation der Benutzermedien.

Sicherheitskarten	MIFARE	LEGIC	Funktionen
Sicherheitskarte C 	✓	—	– Definition Anlagenschlüssel (Sitekey) – Medien konfigurieren – System initialisieren – Applikationen auf leere Karten schreiben.
Sicherheitskarte C1 (IAM) 	—	✓	– Definition des Stamp – System initialisieren – Medien konfigurieren – Segmente erstellen
Sicherheitskarte C2 (SAM) 	—	✓	– Definition des Stamp – System initialisieren – Schreib-Autorisierung für Tischleser und Validierungs-Komponente – Segmente beschreiben.

Schreib-Autorisierung mit der Sicherheitskarte C2
Mit der Sicherheitskarte C2 müssen Komponenten, die Daten in die Segmente auf den Benutzermedien schreiben sollen, eine Schreib-Autorisierung erhalten. Dies sind z.B. Tischleser oder Validierungs-Komponenten. Beschreibung der Anwendung siehe Kapitel Meldungen bei Anwendung der Sicherheitskarte C2 [▸ 8.5].

6.5 Toolkette

Eine Toolkette umfasst die im Subsystem verwendeten Programmierwerkzeuge. Die Werkzeuge verfügen über verschiedene Funktionen zum Konfigurieren, Verwalten, Lesen und Schreiben von Komponenten und Medien.

Tool	Funktionen
Programmer 1460 	• Konfigurieren von Komponenten-Eigenschaften. • Programmieren von Komponenten. • Auslesen des Traceback von Komponenten. • Firmware-Updates an Komponenten. • Inbetriebnahme von Wireless-Komponenten.
Systemsoftware: z. B. dormakaba evolo Manager (KEM). 	• Verwalten von Berechtigungen. • Verwalten von Medien und Personen. • Verwalten von Schließanlagen. • Auswerten von Traceback-Daten.

Tool	Funktionen
Tischleser 91 08 	• Lesen und Schreiben von Medien. • Organisieren des Medienspeichers.
Wireless Gateway 90 40-K7 	• Konfigurieren von Komponenten-Eigenschaften. • Programmieren von Komponenten. • Auslesen des Traceback von Komponenten. • Firmware-Updates an Komponenten.
Wireless Extender 90 41 	• Erweiterung der Funkreichweite des Wireless Gateway. • Für Wireless-Komponenten.
Wireless-Erweiterung am Remoteleser 	91 15 + 90 43 • Wireless-Anbindung für Remoteleser. • CardLink-Update über Wireless.
Mobile Access 	Mobile Access • Verwaltung/Zutritt via Smartphone mit Bluetooth oder NFC.

7 Komponente Programmieren / Konfigurieren

Vor dem Programmieren muss die Medientechnologie festgelegt werden. Siehe Kapitel Medientechnologie festlegen [▸ 7.1].

Durch das anschließende Programmieren / Konfigurieren der Komponente werden Zutrittsrechte und andere Rechte vergeben.

- Wireless-Komponenten benötigen vor dem ersten Einsatz eine Wireless Inbetriebnahme. Siehe Wireless-Dokumentation

7.1 Medientechnologie festlegen

Multi RFID (MRD) Komponenten werden beim ersten Einsatz mit einem Master LEGIC oder MIFARE auf die Technologie festgelegt, in der die Komponenten betrieben werden. Anschließend verhalten sich die Komponenten, wie für die Berechtigungsarten LEGIC (LEA) oder MIFARE (MID) definiert.

Vorgehen

- Das Master-Medium ca. 1 s vor die Antenne halten.
  - Die Medientechnologie des Master-Mediums (Legic- oder MIFARE) wurde auf das Gerät übertragen.

Hinweis: Nach einem INI-Reset muss die Technologie neu festgelegt werden.

7.2 Methoden zur Programmierung und Konfigurierung

Methoden:

- Ohne Hostsystem mit Master- und Benutzer-Medien,
  siehe Kapitel Programmieren mit Medien [▸ 7.4]
- Mit Systemsoftware und Programmer,
  siehe Kapitel Programmieren mit Systemsoftware und Programmer [▸ 7.5.2]
- TouchGo-Produkte:
  siehe Kapitel TouchGo-Produkte programmieren
- Wireless Anwendungen:
  Inbetriebnahme mit Systemsoftware und Programmer,
  danach erfolgt die Konfiguration via wireless Gateway,
  siehe Programmer-, Wireless Gateway-Handbuch und Systembeschreibung
- Mobile Access Geräte: Nach dem Übertragen der Konfiguration mit dem Programmer: Das Gerät für Mobile Access initialisieren,
  siehe Kapitel Initialisieren des Geräts für Mobile Access [▸ 7.6.2].
- evolo smart:
  Die App führt den Benutzer durch den Vorgang.

7.3 TouchGo-Produkte programmieren

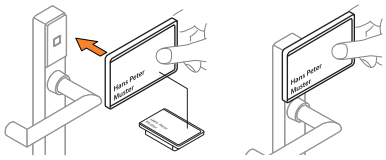
Bei TouchGo wird die Zutrittsberechtigung bei der Berührung der Komponenten geprüft.

Produkt	
c-lever pro TouchGo E110	nur RCID; standalone Whitelist Siehe Bedienungsanleitung dormakaba c-lever pro TouchGo
c-lever pro TouchGo E310	RFID und RCID; evolo SubSystem Siehe Kapitel TouchGo E310 programmieren.

7.3.1 TouchGo E310 programmieren

Beim TouchGo E310 werden für die Programmierung RFID Medien verwendet. Damit die TouchGo Funktion wirksam wird, muss nach der Programmierung ein Pairing von RFID und RCID Benutzermedien erfolgen.

Master-Medien und Benutzermedien des TouchGo E310 wie folgt verwenden:



RFID-Master-Medien und Kombi-Medien (RCID/RFID Benutzermedien) beim TouchGo E310 an die RFID Antenne (Leuchtring) halten.

7.3.1.1 Manuelle Whitelist Programmierung

7.3.1.1.1 Benutzermedien programmieren

Nach dem Vorhalten des Master-B erhält die Komponente folgendes temporäres Recht:

- Dem vorgehaltenen Benutzermedium die Zutrittsberechtigung erteilen (in Whitelist eintragen).

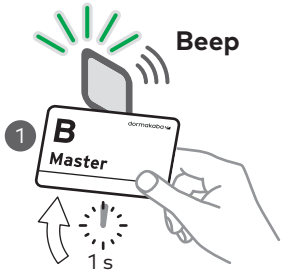
Nach erneutem Vorhalten des Master-B oder nach 20s ohne Vorhalten eines Mediums wird der Komponente das temporäre Recht wieder entzogen.

Voraussetzungen

- A/B-Struktur oder
- B-Struktur ist vorhanden

Vorgehen:

1. Master-B ca. **1 s** vor die Antenne halten.



   ⇨ Grün leuchtet.

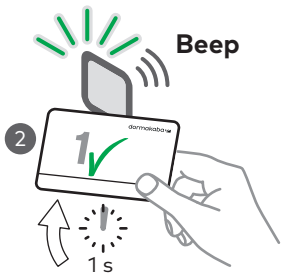
   ⇨ 1 kurzes Signal ertönt.

   ⇨ Grün erlischt.

Wird während 20 s kein Medium vorgehalten, wird der Vorgang automatisch beendet:

-> Die Änderungen wurden übernommen und 1 langes Signal ertönt.

2. Benutzermedium ca. **1 s** vor die Antenne halten.



   ⇨ Grün leuchtet.

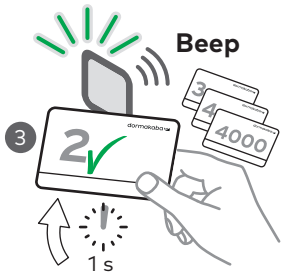
   ⇨ 1 kurzes Signal ertönt.

⇨ Grün erlischt.

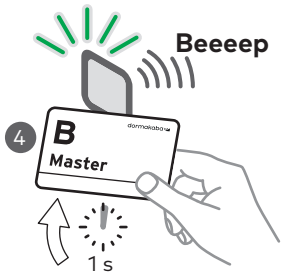
⇨ Das Benutzermedium wurde in die Whitelist eingetragen.

⇨ Das Benutzermedium hat an der Komponente Zutritt.

Weitere Benutzermedien programmieren: Schritt 2 wiederholen.



3. Master-B ca. 1 s vor die Antenne halten.



⇨ Grün leuchtet.

⇨ 1 langes Signal ertönt.

⇨ Grün erlischt.

⇨ Die Änderungen wurden übernommen.

⇨ Das Programmieren ist beendet.

Bei Bedarf mit weiteren Master-B Zutrittsberechtigungen erteilen.

7.3.1.1.2 Einzelne Berechtigung aufheben

Die Zutrittsberechtigung eines Benutzermediums aufheben.

Nach dem Vorhalten des Master-B erhält die Komponente folgendes temporäres Recht:

- Dem vorgehaltenen Benutzermedium die Zutrittsberechtigung entziehen (aus der Whitelist entfernen).

Nach erneutem Vorhalten des Master-B wird der Komponente das temporäre Recht wieder entzogen.

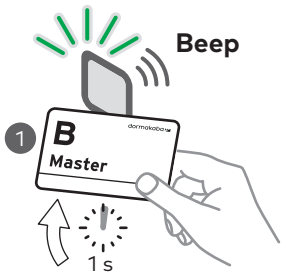
Voraussetzungen

- Benutzermedium mit Zutrittsberechtigung.
- A/B-Struktur oder
- B-Struktur ist vorhanden

Vorgehen

Bei Bedarf weitere Benutzermedien vorhalten.

1. Master-B ca. **1 s** vor die Antenne halten.



⇨ Grün leuchtet.

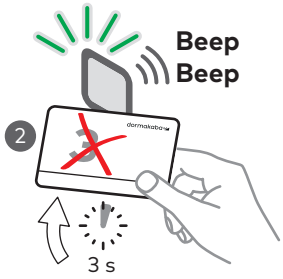
⇨ 1 kurzes Signal ertönt.

⇨ Grün erlischt.

Wird während 20 s kein Medium vorgehalten, wird der Vorgang automatisch beendet:

-> Die Änderungen wurden übernommen und 1 langes Signal ertönt.

2. Benutzermedium ca. **3 s** vor die Antenne halten.



⇨ Grün leuchtet.

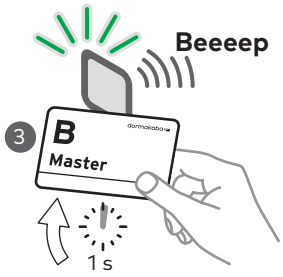
⇨ 2 kurze Signale ertönen.

⇨ Grün erlischt.

⇨ Das Benutzermedium wurde aus der Whitelist entfernt. Das Benutzermedium hat an der Komponente keinen Zutritt.

Bei Bedarf weitere Benutzermedien vorhalten.

3. Master-B ca. 1 s vor die Antenne halten.



⇨ Grün leuchtet.

⇨ 1 langes Signal ertönt.

⇨ Grün erlischt.

⇨ Die Änderungen wurden übernommen.

⇨ Der Vorgang ist beendet.

7.3.1.1.3 Alle Zutrittsberechtigungen aufheben

Nach dem Vorhalten des Master-B erhält die Komponente folgendes temporäres Recht:

- Alle durch den Master-B erteilten Zutrittsberechtigungen aufheben (aus der Whitelist entfernen).

Hinweis: Der Master-B behält das Recht, Zutrittsberechtigungen zu erteilen.

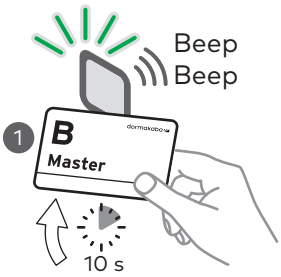
Vorgehen

ACHTUNG

Datenverlust

Wird der Master-B **15 s** vorgehalten, wird ein INI-Reset durchgeführt.
Der INI-Reset löscht alle in der Komponente gespeicherten Einstellungen und Daten.

1. Master-B ca. **10 s** vor die Antenne halten.



   ⇨ Grün leuchtet.

   ⇨ Ab Firmware Version 42: 1 langes und 2 kurze Signale ertönen.
   Vor Firmware Version 42: 2 kurze Signale ertönen.

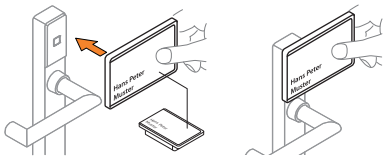
   ⇨ Grün erlischt.

   ⇨ Alle durch den Master-B vergebenen Zutrittsrechte wurden aufgehoben.

⇨ Der Vorgang ist beendet.

7.3.1.2 RCID/RFID Pairing

Der TouchGo E310 wird im dormakaba evolo System verwendet. Für die Programmierung und Identifizierung wird die RFID-Technologie verwendet. Damit die TouchGo Funktion wirksam wird, ist ein Pairing von RFID und RCID Benutzermedien notwendig.



7.3.1.2.1 RCID-Berechtigung erteilen

Whitelist-Berechtigung
Die Berechtigung wird mit dem RFID-Master-Medium und den Kombi-Medien (RCID/RFID Benutzermedien) direkt über die RFID-Antenne programmiert. Beim Lesen des Kombi-Mediums werden die RFID-Daten mit den RCID-Daten (TouchGo) "verheiratet" (Pairing).

CardLink-Berechtigung
Die Berechtigung wird über die Systemsoftware eingerichtet und mit den Kombi-Medien (RFID/RCID Benutzermedien) direkt über die RFID-Antenne angewendet. Beim Lesen des Kombi-Mediums werden die RFID-Daten mit den RCID-Daten (TouchGo) "verheiratet" (Pairing).

Zukünftige Änderungen der Berechtigung und die Aktualisierung der Validierung werden mit der RFID-Technologie an die Komponenten übertragen und gleichzeitig das Pairing geprüft.

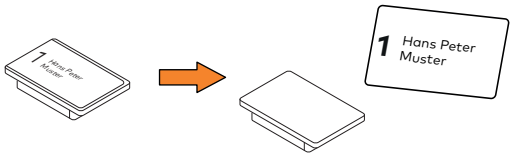
RCID Medien lassen sich nicht doppelt (bereits vorhandenes Pairing) programmieren.

7.3.1.2.2 RCID-Berechtigung aufheben

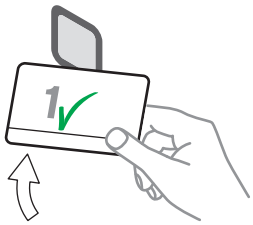
Die RCID-Berechtigung durch Trennen des RCID/RFID Paars aufheben. Dies ist bei Kombi-Medien nicht möglich.

Vorgehen

1. RFID-Medium und RCID-Medium physikalisch trennen.
   Z.B. die Karte aus dem Kartenhalter entnehmen.



2. Das RCID-Medium ca 2 m entfernt auf einem anderen Tisch ablegen.
   ⇨ Das RCID-Medium nicht am Körper tragen.
3. Das RFID-Medium an der Komponente vorhalten.



⇨ Das Pairing ist aufgehoben.

7.3.1.3 TouchGo E310 in Systemsoftware parametrieren

In Schließanlagen, die mit einer Systemsoftware verwaltet werden, können auch TouchGo E310 Komponenten betrieben werden. Die Kombi-Medien (RCID/RFID Benutzermedien) werden mit einem RFID-Master-Medium in die Komponenten programmiert oder die RFID-Daten werden mit dem Tischleser registriert und verwaltet. Die Zutrittsberechtigungen des Kombi-Mediums werden danach mit dem Programmer (Whitelist-Berechtigung) oder den RFID-Daten des Kombi-Mediums (CardLink- Berechtigung) an die Komponenten übertragen.

7.3.1.4 TimePro-Funktion

7.3.1.4.1 Office Mode bei Whitelist

1 Medium mit TimePro:

Die Bedienung ist analog zur Bedienung des Office Mode.
Durch die TimePro-Funktion erfolgt eine zeitgesteuerte Aktivierung.

Mehrere TimePro Einträge:

Aktivierung durch das Kombi-Medium oder durch die TouchGo-Funktion (Innendrücker berühren).
Deaktivierung durch das Kombi-Medium oder das eingestellte Zeitfenster.

7.3.1.4.2 Office Mode bei CardLink

Aktivieren der TimePro-Funktion oder des Office Mode durch das Kombi-Medium oder durch TouchGo (Innendrücker berühren).
Deaktivieren durch das Kombi-Medium oder das eingestellte Zeitfenster.

7.3.1.5 Office Mode Berechtigungen programmieren

Die TouchGo Office Mode Funktion ist im Kapitel Bedienung beschrieben.
Dieses Kapitel beschreibt das Erteilen oder Aufheben der Berechtigung, den Office Mode zu aktivieren oder zu deaktivieren.

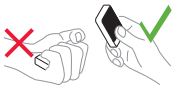
E310
Die Berechtigungen werden mithilfe der Systemsoftware an die Benutzer vergeben.

E110
Programmierung beim TouchGo E110:

- Berechtigung erteilen: Kapitel [▸ 7.3.1.5.1]
- Berechtigung aufheben:
  - Einzelne Berechtigung: Kapitel [▸ 7.3.1.5.2]
  - Alle Berechtigungen: Kapitel [▸ 7.3.1.5.3]

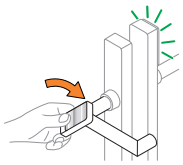
7.3.1.5.1 Office Mode Berechtigung erteilen

- Das Master-Medium und das Benutzermedium nicht mit der Hand umschließen.



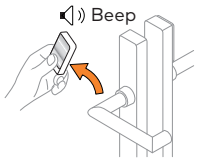
- Nur 1 Medium in die Hand nehmen. Sicherstellen, dass andere Medien mindestens 2 m entfernt sind.

1. Das Master-Medium in die Hand nehmen.
2. Mit dem Zeigefinger den Innendrücker berühren.



⇨ Grün leuchtet.

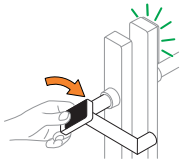
3. Den Zeigefinger/das Master-Medium entfernen..



⇨ Grün erlischt.

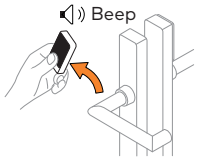
⇨ 1 kurzes Signal ertönt.

4. Das Benutzermedium in die Hand nehmen.
5. Mit dem Zeigefinger den Innendrücker berühren.



⇨ Grün leuchtet.

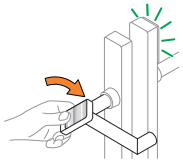
6. Den Zeigefinger/das Benutzermedium entfernen.



⇨ Grün erlischt.

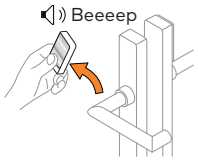
⇨ 1 kurzes Signal ertönt.

7. Das Master-Medium in die Hand nehmen.
8. Mit dem Zeigefinger den Innendrücker berühren.



⇨ Grün leuchtet.

9. Den Zeigefinger/das Master-Medium entfernen.



⇨ Grün erlischt.

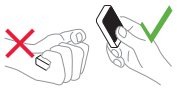
⇨ 1 langes Signal ertönt.

⇨ Die Office Mode Zutrittsberechtigung wurde erteilt.

7.3.1.5.2 Einzelne Office Mode Berechtigung aufheben

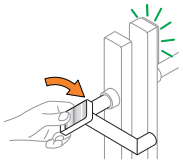
Die Office Mode Berechtigung eines Benutzermediums aufheben.

- Das Master-Medium und das Benutzermedium nicht mit der Hand umschließen.



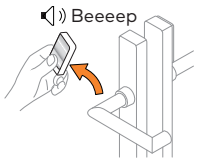
- Nur 1 Medium in die Hand nehmen. Sicherstellen, dass andere Medien mindestens 2 m entfernt sind.

1. Das Master-Medium in die Hand nehmen.
2. Mit dem Zeigefinger den Innendrücker berühren.



⇨ Grün leuchtet.

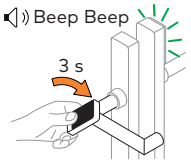
3. Den Zeigefinger/das Medium entfernen.



⇨ Grün erlischt.

⇨ 1 langes Signal ertönt.

4. Das Benutzermedium in die Hand nehmen.
5. Mit dem Zeigefinger den Innendrücker 3 s berühren.

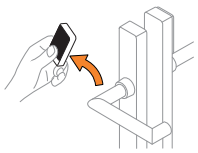


⇨ Grün leuchtet.

⇨ 2 kurze Signale ertönen.

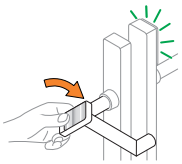
⇨ Die Office Mode Berechtigung des Mediums ist aufgehoben.

6. Den Zeigefinger/das Benutzermedium entfernen.



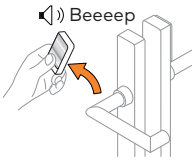
⇨ Grün erlischt.

7. Das Master-Medium in die Hand nehmen.
8. Mit dem Zeigefinger den Innendrücker berühren.



⇨ Grün leuchtet.

9. Den Zeigefinger/das Master-Medium entfernen.



⇨ Grün erlischt.

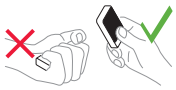
⇨ 1 langes Signal ertönt.

⇨ Die Office-Mode Berechtigung ist aufgehoben.

7.3.1.5.3 Alle Office Mode Berechtigungen aufheben

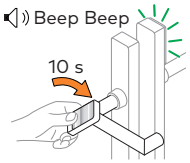
Alle in den Komponenten gespeicherten Office Mode Berechtigungen aufheben.

- Das Master-Medium und das Benutzermedium nicht mit der Hand umschließen.



- Nur 1 Medium in die Hand nehmen. Sicherstellen, dass andere Medien mindestens 2 m entfernt sind.

1. Das Master-Medium in die Hand nehmen.
2. Den Innendrücker 10 s berühren.

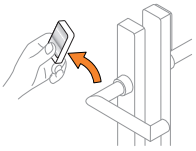


⇨ Grün leuchtet.

⇨ 2 kurze Signale ertönen.

⇨ Alle Berechtigungen sind aufgehoben.

3. Den Zeigefinger/das Master-Medium entfernen.



⇨ Grün erlischt.

⇨ Alle Office-Mode Berechtigungen sind aufgehoben.

7.3.2 Verlorene/defekte Benutzermedien

Die Aufhebung der Berechtigungen verlorener oder defekter Benutzermedien ist für die Anlagensicherheit notwendig. Die Berechtigungen der verbliebenen Benutzermedien werden anschließend neu programmiert.

Ablauf:

1. Alle Berechtigungen aufheben. Siehe [▸ 7.3.1.1.3]
   ⇨ Die Zutrittsberechtigungen werden aufgehoben.
   ⇨ Die Office Mode Berechtigungen werden aufgehoben.
2. Die Benutzermedien neu programmieren.

⇨ Die Zutrittsberechtigungen neu programmieren. Siehe [▸ 7.3.1.1.1]

⇨ Die Office Mode Berechtigungen neu programnmieren. Siehe [▸ 7.3.1.5]

7.4 Programmieren mit Medien



Das Vorhalten eines Master-Mediums (ca. 1 s) aktiviert den Programmier-Modus.

Programmier-Modus verlassen:
Automatisch, 20 s nachdem das letzte Medium vorgehalten wurde (Time-out) oder durch erneutes Vorhalten des Master-Mediums (ca. 1 s).

7.4.1 Karten

7.4.1.1 Oberstes Master-Medium festlegen

- Das oberste Master-Medium ist das oberste Medium einer Komponente.
- Jeder Komponente muss 1 oberstes Master-Medium zugeordnet werden.
- Jeder Komponente kann nur 1 oberstes Master-Medium zugeordnet werden.
- Das erste Master-Medium, das einer Komponente vorgehalten wird, wird als oberstes Master-Medium eingetragen.

A/B Struktur

- In einer A/B-Struktur muss das oberste Master-Medium ein Master-A sein.
- Ein Master-A kann Master-B-Medien Rechte erteilen. Siehe Kapitel "A/B Struktur anlegen".
- Ein Master-A kann Master-B-Medien Rechte entziehen. Siehe Kapitel "Master-B aus der Komponente löschen"
- Mit einem Master-A kann an der Komponente ein INI-Reset gestartet werden, siehe Kapitel "INI-Reset mit Master-Medien"

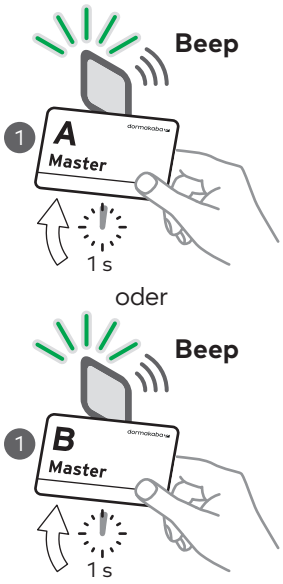
B-Struktur

- In einer B-Struktur muss das oberste Master-Medium ein Master-B sein.
- Mit einem Master-B kann an der Komponente ein INI-Reset gestartet werden, siehe Kapitel "INI-Reset mit Master-Medien"

Voraussetzungen

- Die Komponente befindet sich im Auslieferzustand, siehe INI-Reset.

Vorgehen

	Master-Medium (A oder B) ca. **1 s** vor die Antenne halten. -> Grün leuchtet. -> 1 kurzes Signal ertönt. -> Grün erlischt. -> Das vorgehaltene Master-Medium wurde als oberstes Master-Medium eingetragen.	1x kurz

7.4.1.2 A/B Struktur anlegen

Nach dem Vorhalten des Master-A erhält die Komponente folgendes temporäres Recht:

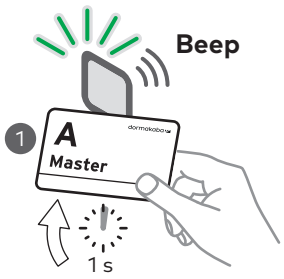
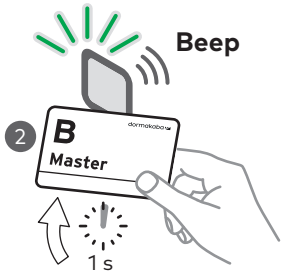
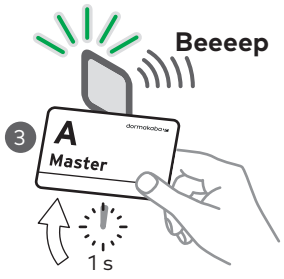
- Den vorgehaltenen Master-B das Recht erteilen, Benutzermedien Zutrittsrechte zu vergeben.

Nach erneutem Vorhalten des Master-A wird der Komponente das temporäre Recht wieder entzogen.

Voraussetzungen

- Der vorgehaltene Master-A ist das oberste Medium der Komponente.
  Siehe Kapitel "Oberstes Master-Medium festlegen"

Vorgehen

	Master-A ca. **1 s** vor die Antenne halten. -> Grün leuchtet. -> 1 kurzes Signal ertönt. -> Grün erlischt.	1x kurz
	Wird während 20 s kein Medium vorgehalten, wird der Vorgang automatisch beendet: -> Die Änderungen wurden übenommen und 1 langes Signal ertönt.	
	Master-B ca. **1 s** vor die Antenne halten. -> Grün leuchtet. -> 1 kurzes Signal ertönt. -> Grün erlischt. -> Master-B hat das Recht, Benutzermedien Zutrittsrechte zu vergeben. -> Die A/B Struktur ist angelegt.	1x kurz
	Bei Bedarf weitere Master-B vorhalten.	
	Master-A ca. **1 s** vor die Antenne halten. -> Grün leuchtet. -> 1 langes Signal ertönt. -> Grün erlischt.	1x lang

7.4.1.3 Zutrittsberechtigungen erteilen

Nach dem Vorhalten des Master-B erhält die Komponente folgendes temporäres Recht:

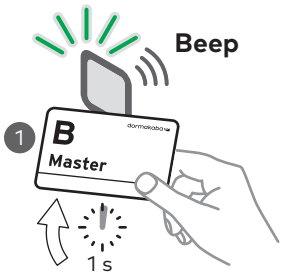
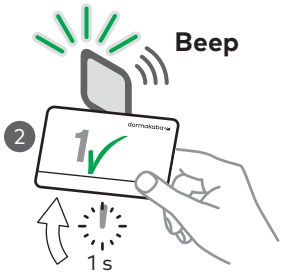
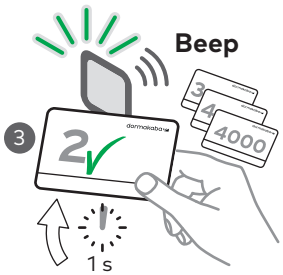
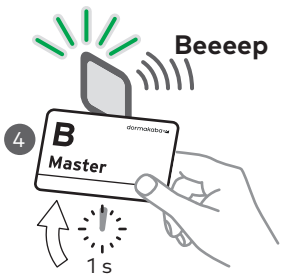
- Dem vorgehaltenen Benutzermedium die Zutrittsberechtigung erteilen (in Whitelist eintragen).

Nach erneutem Vorhalten des Master-B wird der Komponente das temporäre Recht wieder entzogen.

Voraussetzungen

- A/B-Struktur oder
- B-Struktur ist vorhanden

Vorgehen

	Master-B ca. **1 s** vor die Antenne halten. -> Grün leuchtet. -> 1 kurzes Signal ertönt. -> Grün erlischt.	1x kurz
	Wird während 20 s kein Medium vorgehalten, wird der Vorgang automatisch beendet: -> Die Änderungen wurden übenommen und 1 langes Signal ertönt.	
	Benutzermedium ca. **1 s** vor die Antenne halten. -> Grün leuchtet. -> 1 kurzes Signal ertönt. -> Grün erlischt. -> Das Benutzermedium wurde in die Whitelist eingetragen. Das Benutzermedium hat an der Komponente Zutritt.	1x kurz
	Bei Bedarf weitere Benutzermedien in die Whitelist eintragen: Den Handlungschritt 2 wiederholen.	1x kurz
	Master-B ca. 1 s vor die Antenne halten. -> Grün leuchtet. -> 1 langes Signal ertönt. -> Grün erlischt. -> Die Änderungen wurden übenommen.	1x lang
	Bei Bedarf mit weiteren Master-B Zutrittsberechtigungen erteilen.	

7.4.1.4 Einzelne Zutrittsberechtigungen aufheben

Nach dem Vorhalten des Master-B erhält die Komponente folgendes temporäres Recht:

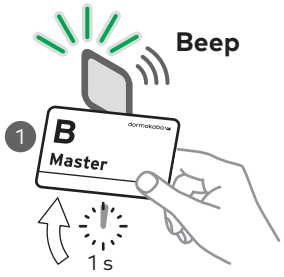
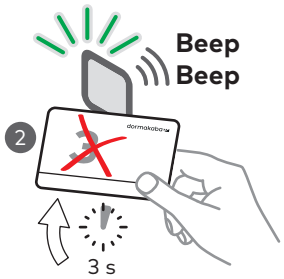
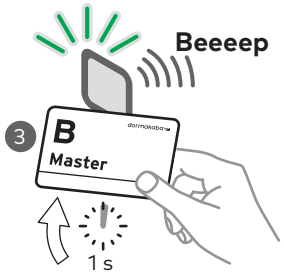
- Dem vorgehaltenen Benutzermedium die Zutrittsberechtigung entziehen (aus der Whitelist entfernen).

Nach erneutem Vorhalten des Master-B wird der Komponente das temporäre Recht wieder entzogen.

Voraussetzungen

- Benutzermedium mit Zutrittsberechtigung.
- A/B-Struktur oder
- B-Struktur ist vorhanden

Vorgehen

	Master-B ca. **1 s** vor die Antenne halten. -> Grün leuchtet. -> 1 kurzes Signal ertönt. -> Grün erlischt.	1x kurz
	Wird während 20 s kein Medium vorgehalten, wird der Vorgang automatisch beendet: -> Die Änderungen wurden übenommen und 1 langes Signal ertönt.	
	Benutzermedium ca. **3 s** vor die Antenne halten. -> Grün leuchtet. -> 2 kurze Signale ertönen. -> Grün erlischt. -> Das Benutzermedium wurde aus der Whitelist entfernt. Das Benutzermedium hat an der Komponente keinen Zutritt. Bei Bedarf weitere Benutzermedien vorhalten.	2x kurz
	Master-B ca. 1 s vor die Antenne halten. -> Grün leuchtet. ->1 langes Signal ertönt. -> Grün erlischt. -> Die Änderungen wurden übenommen.	1x lang

7.4.1.5 Master-B aus der Komponente löschen

Nach dem Vorhalten des Master-A erhält die Komponente folgende temporäre Rechte:

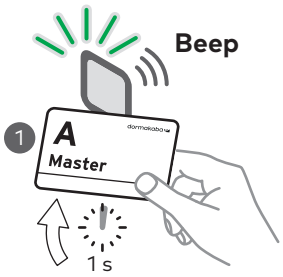
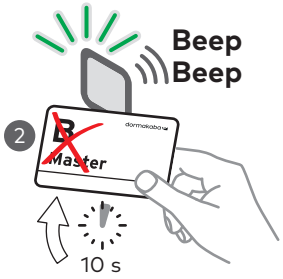
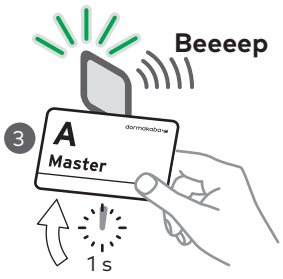
- Alle durch den vorgehaltenen Master-B erteilten Zutrittsberechtigungen aufheben (aus der Whitelist entfernen).
- Dem vorgehaltenen Master-B das Recht entziehen, Zutrittsberechtigungen zu erteilen.

Nach erneutem Vorhalten des Master-A werden der Komponente die temporären Rechte wieder entzogen.

Voraussetzungen

- Der Master-B erhielt seine Rechte durch den Master-A
- A/B-Struktur ist vorhanden

Vorgehen

	Master-A ca. **1 s** vor die Antenne halten. -> Grün leuchtet. -> 1 kurzes Signal ertönt. -> Grün erlischt.	1x kurz
	Wird während 20 s kein Medium vorgehalten, wird der Vorgang automatisch beendet: -> Die Änderungen wurden übenommen und 1 langes Signal ertönt.	
	Master-B vor die Antenne halten (ca. 10 s), bis 2 kurze Signale ertönen. -> Grün leuchtet solange der Master-B vorgehalten wird. Bei Bedarf weitere Master-B vorhalten.	2x kurz
	Master-A ca. **1 s** vor die Antenne halten. -> Grün leuchtet. -> 1 langes Signal ertönt. -> Grün erlischt. -> Die Änderungen wurden übenommen.	1x lang

7.4.1.6 Alle durch Master-B vergebenen Zutrittsberechtigungen aufheben

Nach dem Vorhalten des Master-B erhält die Komponente folgendes temporäres Recht:

- Alle durch den Master-B erteilten Zutrittsberechtigungen aufheben (aus der Whitelist entfernen).

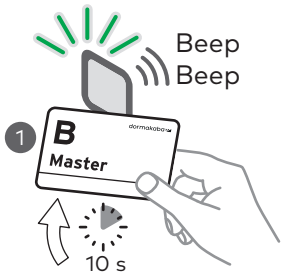
Hinweis: Der Master-B behält das Recht, Zutrittsberechtigungen zu erteilen.

Vorgehen

ACHTUNG

Datenverlust

Wird der Master-B **15 s** vorgehalten, wird ein INI-Reset durchgeführt.
Der INI-Reset löscht alle in der Komponente gespeicherten Einstellungen und Daten.

	Master-B ca. **10 s** vor die Antenne halten. -> Grün leuchtet. -> 1 langes und 1 kurzes Signal ertönen (ab Firmware Version 42). -> (vor Firmware Version 42: 2 kurze Signale ertönen.) -> Grün erlischt. -> Alle durch den Master-B vergebenen Zutrittsrechte wurden aufgehoben.	Ab Firmware Version 42: 1x lang 1x kurz Vor Firmware Version 42: 2x kurz

7.4.2 Schlüssel

7.4.2.1 Oberstes Master-Medium festlegen

- Das oberste Master-Medium ist das oberste Medium einer Komponente.
- Jeder Komponente muss 1 oberstes Master-Medium zugeordnet werden.
- Jeder Komponente kann nur 1 oberstes Master-Medium zugeordnet werden.
- Das erste Master-Medium, das in den Zylinder eingesteckt wird, wird als oberstes Master-Medium eingetragen.

A/B Struktur

- In einer A/B-Struktur muss das oberste Master-Medium ein Master-A sein.
- Ein Master-A kann Master-B-Medien Rechte erteilen. Siehe Kapitel "A/B Struktur anlegen".
- Ein Master-A kann Master-B-Medien Rechte entziehen. Siehe Kapitel "Master-B aus der Komponente löschen"
- Mit einem Master-A kann an der Komponente ein INI-Reset gestartet werden, siehe Kapitel "INI-Reset mit Master-Medien"

B-Struktur

- In einer B-Struktur muss das oberste Master-Medium ein Master-B sein.
- Mit einem Master-B kann an der Komponente ein INI-Reset gestartet werden, siehe Kapitel "INI-Reset mit Master-Medien".

Voraussetzungen

- Die Komponente befindet sich im Auslieferzustand, siehe INI-Reset.

Vorgehen

Master A Beep 1 1 s oder Master B Beep 1 1 s	Master-Medium (A oder B) ca. **1 s** in den Zylinder einstecken. -> 1 kurzes Signal ertönt. -> Das vorgehaltene Master-Medium wurde als oberstes Master-Medium eingetragen.	1x kurz

7.4.2.2 A/B Struktur anlegen

Nach dem Einstecken des Master-A erhält die Komponente folgendes temporäres Recht:

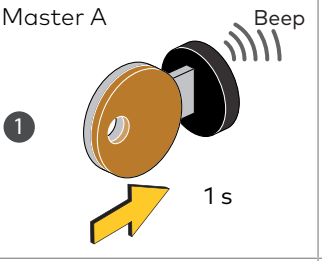
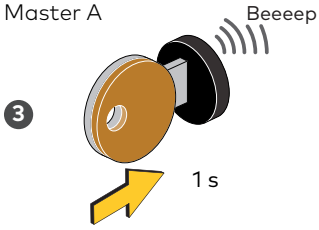
- Dem in den Zylinder eingesteckten Master-B das Recht erteilen, Benutzermedien Zutrittsrechte zu vergeben.

Nach erneutem Einstecken des Master-A wird der Komponente das temporäre Recht wieder entzogen.

Voraussetzungen

- Der in den Zylinder eingesteckte Master-A ist das oberste Medium der Komponente. Siehe Kapitel "Oberstes Master-Medium festlegen"

Vorgehen

Master A Beep  	Master-A ca. **1 s** in den Zylinder einstecken. -> 1 kurzes Signal ertönt.	1x kurz
	Wird während 20 s kein Medium in den Zylinder eingesteckt, wird der Vorgang automatisch beendet: -> Die Änderungen wurden übenommen und 1 langes Signal ertönt.	
Master B Beep  	Master-B ca. **1 s** in den Zylinder einstecken. -> 1 kurzes Signal ertönt. -> Master-B hat das Recht, Benutzermedien Zutrittsrechte zu vergeben. -> Die A/B Struktur ist angelegt.	1x kurz
	Bei Bedarf weitere Master-B vorhalten.	
Master A Beeeep  	Master-A ca. **1 s** in den Zylinder einstecken. -> 1 langes Signal ertönt.	1x lang

7.4.2.3 Zutrittsberechtigungen erteilen

Nach dem Einstecken des Master-B erhält die Komponente folgendes temporäres Recht:

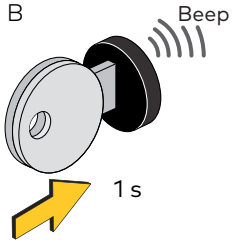
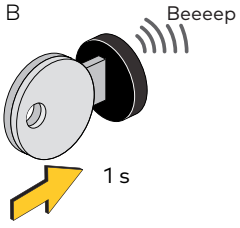
- Dem in den Zylinder eingesteckten Benutzermedium die Zutrittsberechtigung erteilen (in Whitelist eintragen).

Nach erneutem Einstecken des Master-B wird der Komponente das temporäre Recht wieder entzogen.

Voraussetzungen

- A/B-Struktur oder
- B-Struktur ist vorhanden

Vorgehen

Master B Beep 1 	Master-B ca. **1 s** in den Zylinder einstecken. -> 1 kurzes Signal ertönt.	1x kurz
	Wird während 20 s kein Medium in den Zylinder eingesteckt, wird der Vorgang automatisch beendet: -> Die Änderungen wurden übenommen und 1 langes Signal ertönt.	
User 1 Beep 2 	Benutzermedium ca. **1 s** in den Zylinder einstecken. -> 1 kurzes Signal ertönt. -> Das Benutzermedium wurde in die Whitelist eingetragen. Das Benutzermedium hat an der Komponente Zutritt.	1x kurz
User 2,3 ... Beep 3 	Bei Bedarf weitere Benutzermedien in die Whitelist eintragen: Den Handlungschritt 2 wiederholen.	1x kurz
Master B Beeeep 4 	Master-B ca. 1 s in den Zylinder einstecken. -> 1 langes Signal ertönt. -> Die Änderungen wurden übenommen.	1x lang
	Bei Bedarf mit weiteren Master-B Zutrittsberechtigungen erteilen.	

7.4.2.4 Einzelne Zutrittsberechtigungen aufheben

Nach dem Einstecken des Master-B erhält die Komponente folgendes temporäres Recht:

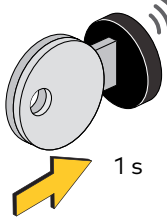
- Dem in den Zylinder eingesteckten Benutzermedium die Zutrittsberechtigung entziehen (aus der Whitelist entfernen).

Nach erneutem Einstecken des Master-B wird der Komponente das temporäre Recht wieder entzogen.

Voraussetzungen

- Benutzermedium mit Zutrittsberechtigung.
- A/B-Struktur oder
- B-Struktur ist vorhanden

Vorgehen

Master B Beep 1  	Master-B ca. **1 s** in den Zylinder einstecken. -> 1 kurzes Signal ertönt.	1x kurz
	Wird während 20 s kein Medium in den Zylinder eingesteckt, wird der Vorgang automatisch beendet: -> Die Änderungen wurden übenommen und 1 langes Signal ertönt.	
User Beep Beep 2  	Benutzermedium ca. **3 s** in den Zylinder einstecken. -> 2 kurze Signale ertönen.. -> Das Benutzermedium wurde aus der Whitelist entfernt. Das Benutzermedium hat an der Komponente keinen Zutritt. Bei Bedarf weitere Benutzermedien vorhalten.	2x kurz
Master B Beeeep 3  	Master-B ca. 1 s in den Zylinder einstecken. ->1 langes Signal ertönt. -> Die Änderungen wurden übenommen.	1x lang

7.4.2.5 Master-B aus der Komponente löschen

Nach dem Einstecken des Master-A erhält die Komponente folgende temporäre Rechte:

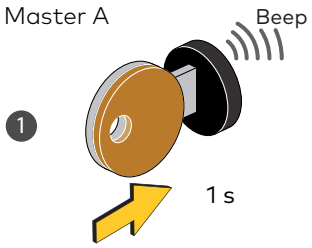
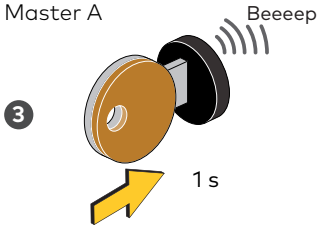
- Alle durch den eingesteckten Master-B erteilten Zutrittsberechtigungen aufheben (aus der Whitelist entfernen).
- Dem eingesteckten Master-B das Recht entziehen, Zutrittsberechtigungen zu erteilen.

Nach erneutem Einstecken des Master-A werden der Komponente die temporären Rechte wieder entzogen.

Voraussetzungen

- Der Master-B erhielt seine Rechte durch den Master-A
- A/B-Struktur ist vorhanden

Vorgehen

Master A Beep  	Master-A ca. **1 s** in den Zylinder einstecken. -> 1 kurzes Signal ertönt.	1x kurz
	Wird während 20 s kein Medium in den Zylinder eingesteckt, wird der Vorgang automatisch beendet: -> Die Änderungen wurden übenommen und 1 langes Signal ertönt.	
Master B Beep Beep  	Master-B in den Zylinder einstecken (ca. 10 s), bis 2 kurze Signale ertönen. Bei Bedarf weitere Master-B vorhalten.	2x kurz
Master A Beeeep  	Master-A ca. **1 s** in den Zylinder einstecken. -> 1 langes Signal ertönt. -> Die Änderungen wurden übenommen.	1x lang

7.4.2.6 Alle durch Master-B vergebenen Zutrittsberechtigungen aufheben

Nach dem Einstecken des Master-B erhält die Komponente folgendes temporäres Recht:

- Alle durch den Master-B erteilten Zutrittsberechtigungen aufheben (aus der Whitelist entfernen).

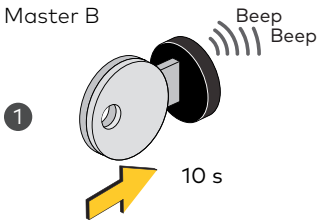
Hinweis: Der Master-B behält das Recht, Zutrittsberechtigungen zu erteilen.

Vorgehen

ACHTUNG

Datenverlust

Ist der Master-B **15 s** eingesteckt, startet der INI-Reset.
Der INI-Reset löscht alle in der Komponente gespeicherten Einstellungen und Daten.

	Master-B ca. **10 s** in den Zylinder einstecken. -> 1 langes und 2 kurze Signale ertönen (ab Firmware Version 42). -> (vor Firmware Version 42: 2 kurze Signale ertönen.). -> Alle durch den Master-B vergebenen Zutrittsrechte wurden aufgehoben.	Ab Firmware Version 42: 1x lang 1x kurz Vor Firmware Version 42: 2x kurz

7.4.3 INI-Reset mit Master-Medien

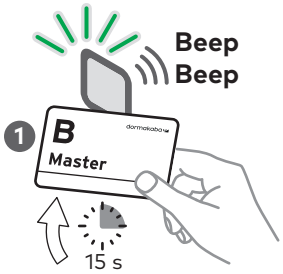
Auswirkungen des INI-Resets

- Parametrierungen und Daten werden gelöscht und auf die Ausgangswerte (Werkseinstellung) zurückgesetzt.
- Der Durchgang ist während des INI-Resets gesperrt.
- Alle Zutritsberechtigungen, Master-Medien und das Traceback werden gelöscht.
- Der Durchgang ist nach dem INI-Reset gesperrt.

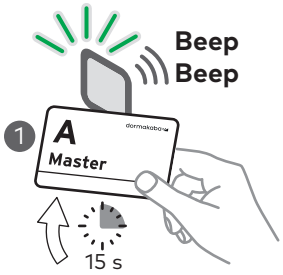
7.4.3.1 Karten

7.4.3.1.1 Whitelist

In Master-B-Struktur

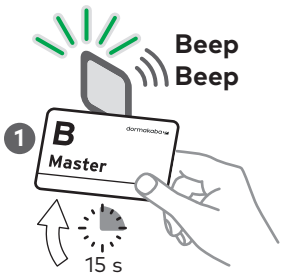
INI-Reset mit Master-B		
	Master-B ca. **15 s** vor die Antenne halten. -> Grün leuchtet. -> Nebenstehende Signale ertönen. -> Nach 15 s wird der INI-Reset ausgeführt. -> Grün erlischt.	nach 10 s: 1x lang, 1x kurz, nach 15 s, 2x kurz

In Master-A/B-Struktur

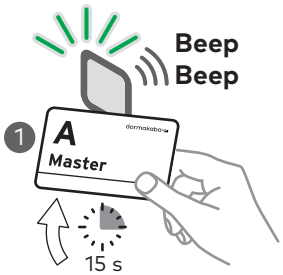
INI-Reset mit Master-A		
	Master-A ca. **15 s** vor die Antenne halten. -> Grün leuchtet. -> Nebenstehende Signale ertönen. -> Nach 15 s wird der INI-Reset ausgeführt. -> Grün erlischt.	nach 10 s: 1x lang, 1x kurz, nach 15 s, 2x kurz

7.4.3.1.2 Cardlink

Mit Master-B

INI-Reset mit Master-B		
	Master-B ca. **15 s** vor die Antenne halten. -> Grün leuchtet. -> Nach 15 s wird der INI-Reset ausgeführt. -> 2 kurze Signale ertönen. -> Grün erlischt.	2x kurz

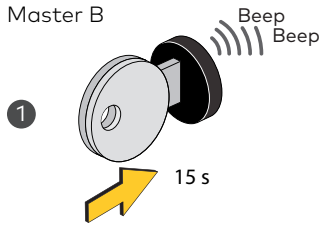
Mit Master-A

INI-Reset mit Master-A		
	Master-A ca. **15 s** vor die Antenne halten. -> Grün leuchtet. -> Nach 15 s wird der INI-Reset ausgeführt. -> 2 kurze Signale ertönen. -> Grün erlischt.	2x kurz

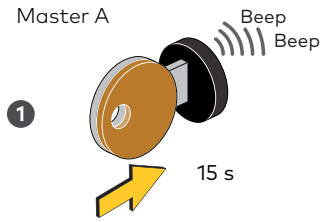
7.4.3.2 Schlüssel

7.4.3.2.1 Whitelist

In Master-B-Struktur

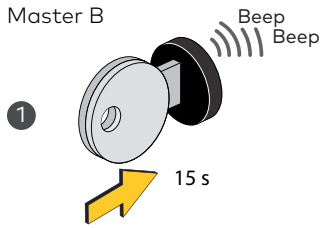
INI-Reset mit Master-B		
	Master-B ca. **15 s** in den Zylinder einstecken. -> Nebenstehende Signale ertönen. -> Nach 15 s wird der INI-Reset ausgeführt.	nach 10 s: 1x lang, 1x kurz, nach 15 s, 2x kurz

In Master-A/B-Struktur

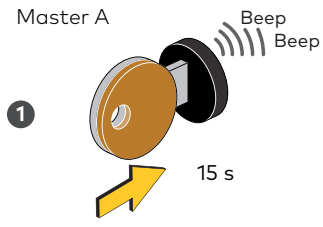
INI-Reset mit Master-A		
	Master-A ca. **15 s** in den Zylinder einstecken. -> Nebenstehende Signale ertönen. -> Nach 15 s wird der INI-Reset ausgeführt.	nach 10 s: 1x lang, 1x kurz, nach 15 s, 2x kurz

7.4.3.2.2 Cardlink

Mit Master-B

INI-Reset mit Master-B		
	Master-B ca. **15 s** in den Zylinder einstecken. -> Nach 15 s wird der INI-Reset ausgeführt. -> 2 kurze Signale ertönen.	2x kurz

Mit Master-A

INI-Reset mit Master-A		
	Master-A ca. **15 s** in den Zylinder einstecken. -> Nach 15 s wird der INI-Reset ausgeführt. -> 2 kurze Signale ertönen.	2x kurz

7.5 Programmieren mit Systemsoftware

Mit dieser Programmierart werden die Daten, die in der Systemsoftware konfiguriert wurden, mit dem Programmer oder über Wireless auf die Komponenten übertragen. Für diese Programmierart werden die Master-Medien der Schließanlage zwingend benötigt. Bei Wireless-Betrieb werden die Master-Medien für die Inbetriebnaheme der Komponenten benötigt. Das Programmieren von Zeitfunktionen und das Auslesen des Traceback (Ereignisspeicher) sind mit dieser Programmierart möglich.

Mit der Systemsoftware werden Komponenten und Medien verwaltet, sowie Berechtigungen vergeben. Dabei können eine Vielzahl von organisatorischen, baulichen und personellen Gegebenheiten abgebildet und alle Bewegungen rückverfolgt werden.

7.5.1 Systemsoftware für evolo Komponenten

Je nach Einsatzbereich und Anlagengröße wird verschiedene Systemsoftware eingesetzt.

7.5.2 Programmieren mit Systemsoftware und Programmer

Vorgehen

- In der Systemsoftware das Gerät konfigurieren.
- Die Konfiguration auf den Programmer übertragen.
- Das Master-Medium ca. 1 s vor die Antenne halten.
- Den Programmer mit dem Gerät verbinden.
- Die Konfiguration vom Programmer auf das Gerät übertragen.

Siehe auch:

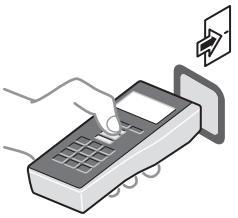
- Systembeschreibung
- Dokumentation der eingesetzten Systemsoftware
- Bedienungsanleitung Programmer 1460
- Planungsrichtlinie Wireless

7.5.3 Export in Komponenten

Beim Export werden die Konfigurationsdaten vom Programmer in die Komponenten übertragen.

Für den Export sind zuerst die Konfigurationsdaten der Schließpläne von der Systemsoftware auf den Programmer zu übertragen.

7.5.3.1 Export in evolo Komponenten



Aus der Liste im Programmer sind die Konfigurationsdaten auszuwählen und in die Komponenten zu exportieren.

✓ Gültiges Master-Medium vorhanden

1. Menü Taste Export drücken.
   ⇨ Das Menü Export öffnet.
2. Master an der Komponente anmelden.

Die Elektronik des Schrankschlosses 21 10 durch kurzes Andrücken der Tür aktivieren.

3. Schließplan wählen.
4. Taste ENTER drücken.
5. Aktuator wählen.
6. Taste ENTER drücken.

7.5.4 Import aus Komponenten

Die Elektronik des Schrankschlosses 21 10 durch kurzes Andrücken der Tür aktivieren.

Beim Import werden die Konfigurationsdaten aus den Komponenten in den Programmer übertragen. Anschließend wird der Programmer an einen PC angeschlossen, um die Daten mit einem Hostsystem z. B. in der Traceback-Analyse weiter zu verarbeiten oder ein Support-Paket zu erstellen, das dem Support bei der Fehleranalyse hilft.

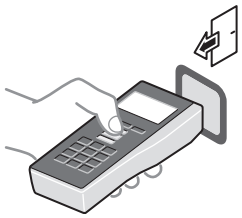
Es stehen folgende Daten zur Auswahl:

- Info (Statusdaten)
- Traceback
- Konfiguration
- CardLink Update
- Diagnosedaten

Bestehende Konfigurationsdaten von Komponenten werden nach der Bestätigung auf dem Programmer überschrieben.

Das Traceback und die Konfiguration müssen für die Auswertung mit dem Programmer in die Systemsoftware übertragen werden.

7.5.4.1 Import aus Digitalzylinder, c-lever und Leser



✓ Gültiges Master-Medium vorhanden

1. Menü Taste Import drücken.
   ⇨ Das Menü Import öffnet.
2. Master an der Komponente anmelden.

Die Elektronik des Schrankschlosses 21 10 durch kurzes Andrücken der Tür aktivieren.

3. Menü, z.B. Konfiguration wählen.
4. Taste ENTER drücken.

⇨ Die Konfiguration der Komponente wird ausgelesen und bestätigt.

7.6 Mobile Access

7.6.1 Systemvoraussetzungen

Firmware/Systemsoftware

Funktion	Firmware	Systemsoftware		
		Kaba exos 9300	**MATRIX**	**KEM**
Mobile Access	Siehe Kapitel Gültigkeit > Option Mobile Access	Ab Version 4.0.73	MATRIX Professional Ab Version 3.2.x, mit Option Mobile Access MATRIX ONE Ab Version 3.7	Ab Version 6.0

7.6.2 Initialisieren des Geräts für Mobile Access

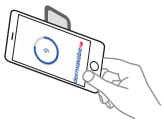
Voraussetzungen

Allgemein	• Die Zutrittskontrollanlage ist von domakaba bei Legic Connect eingerichtet
Systemsoftware	• Die installierte Version der Systemsoftware unterstützt Mobile Access. • Eine Verbindung zu Legic Connect ist eingerichtet. • Das Gerät ist in der Systemsoftware für Mobile Access konfiguriert. • Die Konfiguration ist auf den Programmer übertragen.
Gerät	• Das Gerät ist installiert und betriebsbereit. • Die Medientechnologie ist festgelegt, siehe Kapitel Medientechnologie festlegen • Die Konfiguration ist vom Programmer auf das Gerät übertragen.
Smartphone	• Der VCP Installer ist installiert und bei Legic Connect mit der Telefonnummer registriert. Der per SMS erhaltene Registrierungscode ist eingegeben. • Der Zugriff auf das Internet ist möglich (WLAN oder Mobile Daten). • Das Passwort für die VCP-Datei ist bekannt.

Vorgehen

Bluetooth/NFC Schlüssel auf das Gerät übertragen

- Das Master-Medium ca. 1 s vor die Antenne halten.
- Auf dem Smartphone den VCP Installer starten.
- Die VCP-Datei auswählen.
  - Ist die gewünschte VCP-Datei nicht vorhanden, 'Aktualisieren' auswählen. Danach lädt das Smartphone die VCP-Datei herunter.
- Auf 'Senden' tippen.
- Das Passwort für die VCP-Datei eingeben.



- Das Smartphone vor das Lesegerät halten.

Signalisierung / Anzeige		
	Gerät / Antenne	**Smartphone**
Während der Datenübertragung:	• Grün leuchtet.	
Nach erfolgreicher Initialisierung:	• 3 Signale ertönen.	• Grün • Seriennummer des Geräts
Das Gerät ist initialisiert.		
Nach nicht erfolgreicher Initialisierung:	• 1 kurzes Signal ertönt. • Rot leuchtet kurz. • 1 langes Signal ertönt. • Rot leuchtet kurz. • 1 kurzes Signal ertönt.	• Rot

7.6.3 Initialisieren des Geräts für evolo smart

Die evolo smart App leitet den Benutzer durch den Vorgang zur Initialisierung der Komponente.

7.6.4 Bluetooth Signalstärke einstellen

Die Default-Werte nur dann verändern, wenn dies zwingend notwendig ist.

- Geräte ohne wireless Anbindung:
  Im übergeordneten System die Bluetooth Signalstärke einstellen und mit Hilfe des Programmer auf das Gerät übertragen.
- Geräte mit wireless Anbindung:
  Im übergeordneten System die Bluetooth Signalstärke einstellen und via Wireless Gateway auf das Gerät übertragen.

Siehe auch Planungsrichtline Mobile Access.

7.7 Initialisieren von Wireless-Komponenten

Damit die Komponenten im Wireless-Betrieb arbeiten können, muss eine Wireless-Inbetriebnahme durchgeführt werden.

Weitere Informationen zu Wireless befinden sich in der Planungsrichtlinie Wireless und im technischen Handbuch zum Gateway 90 40-K7.

Voraussetzungen

- Das betreffende Gateway ist in der Systemsoftware angelegt und konfiguriert.
- Die Komponente ist in der Systemsoftware angelegt.
- Die Komponente ist für den Wireless-Betrieb konfiguriert.

Beim Betrieb mit mehreren Gateways die Wireless-Inbetriebnahme immer nur auf einem Gateway starten.
Die Komponenten könnten sich sonst mit einem unerwünschten Gateway verbinden.

Starten der Wireless-Inbetriebnahme auf dem Gateway:
Via Web-Interface

1. Im Dateimanager das Gateway für die Inbetriebnahme auswählen.
2. Das Web-Interface des Gateway starten.
3. Die Funktion 'Wireless Inbetriebnahme' aufrufen.
4. Die Zeitspanne für die Inbetriebnahme einstellen.
   ⇨ Während dieser Zeitspanne können die Komponenten mit dem Gateway verbunden werden.
5. Die Wireless-Inbetriebnahme starten.

Via Systemsoftware

✓ Das Gateway für die Inbetriebnahme ist in der Systemsoftware angelegt und konfiguriert.

1. In der Systemsoftware das Gateway für die Inbetriebnahme auswählen.
2. Die Funktion 'Wireless Inbetriebnahme' aufrufen.
3. Die Zeitspanne für die Inbetriebnahme einstellen.
   ⇨ Während dieser Zeitspanne können die Komponenten mit dem Gateway verbunden werden.
4. Die Wireless-Inbetriebnahme starten.

Wenn nicht alle benötigten Komponenten innerhalb der eingestellten Zeitspanne in Betrieb genommen werden konnten, kann der Vorgang wiederholt werden. Bereits mit dem Gateway verbundene Komponenten bleiben verbunden.

Komponente verbinden

✓ Das Gateway ist angelegt.

✓ Die Wireless Konfiguration der Komponente ist auf den Programmer übertragen worden oder die Komponente ist bereits für den Wireless Betrieb konfiguriert.

✓ Die Wireless Inbetriebnahme auf dem Gateway ist gestartet.

1. Mit dem Master-Medium an der Komponente anmelden.

2. Im Programmer das Menü 'Einstellungen Aktuator' öffnen.
3. Das Untermenü Wireless wählen.
4. **Verbinden** wählen.
5. Bestätigen mit ENTER.
   - ⇨ Netzwerk suchen ... (Netzwerk wird gesucht.)
   - ⇨ Gateway (GW) gefunden.
   - ⇨ Verbinden mit dem GW wird ausgeführt.
   - ⇨ Inbetriebnahme ...
   - ⇨ Mit GW verbunden.

⇨ Die Wireless Inbetriebnahme des Geräts ist abgeschlossen.

7.8 Eigenschaften und Funktionen einer Komponente einstellen

Mit dem Programmer können folgende Eigenschaften einer Komponente verändert werden:

- Das Datum und die Uhrzeit der Uhr.
- Die akustische und optische Anzeige.
- Die Öffnungszeit (Default-Wert 6 s).
- Die Firmware-Version.
- Der INI-Reset.
- Eine Wireless Komponente mit einem wireless Gateway verbinden.

Hauptfunktionen
Die beiden Hauptfunktionen, die mit dem Programmer an Komponenten ausgeführt werden können, sind **Export** und **Import** von Daten. Beide Funktionen werden mit dem Programmer über die Funkschnittstelle (NFC) oder mit dem Programmierkabel durchgeführt.

7.9 Reset (INI-Reset)

Mit einem INI-Reset lassen sich die Komponenten in den Lieferzustand zurücksetzen.

ACHTUNG

Datenverlust

Bei einem INI-Reset werden alle bisher gespeicherten Einstellungen und Daten auf dem E-Modul gelöscht.

Bei Wireless-Komponenten wird die Verbindung zum Gateway getrennt.

Dafür stehen folgende Möglichkeiten zur Verfügung:

Reset mit Master-Medien
Ein INI-Reset wird ausgeführt, wenn das jeweilige Master-Medium den Komponenten vor die Antenne gehalten wird.

Reset mit Programmer 1460
Ein INI-Reset kann auch mit dem Programmer vorgenommen werden. Für diese Variante wird zusätzlich das jeweilige Master-Medium benötigt.

Reset mit Pinzette und gültigen Master-Medien
Einige Komponenten verfügen über INI-Reset-Kontakte auf dem E-Modul. Diese Kontakte mit einer elektrisch leitenden Pinzette kurzschließen und ein INI-Reset wird ausgeführt.

Reset mit DIP-Schalter
Einige Komponenten verfügen über DIP-Schalter. Den spezifischen DIP-Schalter einschalten und ein INI-Reset wird ausgeführt.

Weitere Informationen zum INI-Reset sind in der Dokumentation der Komponente beschrieben.

7.9.1 Übersicht der INI-Reset-Varianten der Komponenten

In der folgenden Tabelle werden die INI-Reset-Varianten und die Unterschiede für E300 (V4) und V3 aufgeführt.

Einige Komponenten verfügen über INI-Reset-Kontakte. Diese Kontakte mit einer elektrisch leitenden Pinzette für ca. 3 Sekunden kurzschließen, um einen INI-Reset auszuführen.

Komponente	Admin Master	Programmer 1460[1]	Pinzette	DIP-Schalter
c-lever	✓	✓	✓	—
c-lever pro	✓	✓	✓	—
c-lever pro TouchGo	✓	—	✓	—
c-lever compact	✓	✓	—	—
Digitalzylinder	✓	✓	✓[2]	—
Mechatronikzylinder Stulp	✓	✓	—[4]	—
Mechatronikzylinder Aufsatz/ Kompakt	✓	✓	✓[2]	—
Remoteleser	✓	✓	—	✓[3]
Kompaktleser	✓	✓	—	✓[3]
Schrankschloss 21 10	✓	✓[2]	✓	—

Legende:

1 Master-Medium davor halten.

2 Master-Medium oder berechtigtes Benutzermedium davor halten.

3 DIP-Schalter 6 auf ON stellen.

4 Resetpunkte im Stulp-Modul

Reset-Informationen für weitere Komponenten sind in den Handbüchern der Komponenten beschrieben.



Einen INI-Reset immer gemäß Gerätehandbuch durchführen.

7.10 Energie sparen

Standalone-Komponenten

Die Energiemenge der Batterie und der Energieverbrauch bestimmen bei Standalone-Komponenten, wie lange diese arbeiten können, bevor der Energievorrat erschöpft ist. Durch verschiedene Einstellmöglichkeiten kann Energie eingespart werden.

7.10.1 Funktionen deaktivieren

Zum Energiesparen nicht benötigte Funktionen deaktivieren.

Abhängig vom Gerätetyp und dem Einsatz können eine oder mehrere Funktionen deaktiviert werden, wenn sie für den Einsatzzweck nicht benötigt werden. Dies hilft, Energie einzusparen und den Zeitraum zwischen 2 Batteriewechseln zu verlängern.

Beispiele für Funktionen, die deaktiviert werden können:

- akustische Signalisierung (Buzzer)
- optische Signalisierung (Leuchtring)

- Medientraceback
- Nicht benötigte Technologien
- Wireless Funktion (wenn nicht benötigt)
- Wireless Sendeleistung reduzieren, wenn möglich.
- Mobile Access (Wenn nicht benötigt)

7.10.2 Funktion Object in Field

Die Komponente überprüft in regelmäßigen Abständen, ob sich ein Medium im Antennenfeld befindet. Um Energie zu sparen wird die Zeitspanne zwischen zwei Überprüfungen verlängert. Bei dynamischem "Object in Field" wird diese Zeitspanne schrittweise bis zum Maximalwert weiter ausgedehnt. Wird ein Medium vorgehalten, beginnt der Vorgang erneut. Beim Vorhalten eines Mediums ist eine längere Reaktionszeit möglich.

Die Funktion "Object in Field" (OIF) wird in der Systemsoftware parametriert.

Tabelle: Energieeinsparung durch dynamisches OIF. Die Werte sind Näherungswerte. Tatsächliche Energieeinsparungen sind noch von weiteren Faktoren und Einstellungen abhängig.

Anwendungsfall	**Einstellungen**		**Einspa-rung**	**Auswirkungen**
Beispiele	**OiF Intervall**	**Dyn. OiF**	**maximal**	
Standardeinstellung der Komponente. **Stark frequentierte Zugänge**	300 ms	AUS	0%	Normal
Wenig frequentierte Zugänge	300 ms	EIN 30 min	15%	Verlängerte Reaktionszeit beim ersten vorgehaltenen Medium nach längerer Pause. Bei weiteren Medien innerhalb der eingestellten Zeit normal.
• Je 20 Vorgänge morgens und abends Innerhalb der eingestellten Zeit. Dazwischen während 10 Stunden 1 Vorgang pro Stunde.	300 ms	EIN 30 min	19%	
• Während 10 Stunden 1 Vorgang pro Stunde	300 ms	EIN 30 min	22%	
Selten benötigte Zugänge • 2 Vorgänge morgens und 2 abends innerhalb der eingestellten Zeit. Dazwischen keine Vorgänge.	300 ms	EIN 30 min	30%	Verlängerte Reaktionszeit bei der ersten Nutzung nach längerer Pause. • Das Auslesen eines vorgehaltenen Mediums kann bis zu 1 s dauern.
• Lange Ruhezeiten zwischen den Vorgängen • einen oder mehrere Tage kein Vorgang	1000 ms	AUS	34%	

8 Signale

Das Kapitel beschreibt die beiden Signalarten, deren Bedeutung und die jeweiligen Meldungen.

Akustische Signale und optische Anzeigen werden ausgegeben, wenn Medien von der Antenne der Komponente erkannt werden.
Die Signale und Anzeigen für Zutrittsberechtigung sind mit der Toolkette individuell aktivierbar oder deaktivierbar.

Symbole

Symbole		Beschreibung
		Akustisches Signal
		Optisches Signal

8.1 Signaldauer

Beim Vorweisen von Benutzermedien mit einer Zutrittsberechtigung werden folgende akustische Signale (Beep) und optische Anzeigen (LED) ausgegeben.

Signale / Anzeigen	Dauer	Dauer
Beep / LED leuchtet	sehr kurz	40 ms
Beep / LED leuchtet	kurz	120 ms
Beep / LED leuchtet	lang	600 ms
Beep / LED leuchtet	sehr lang	3000 ms

8.2 Zutrittsberechtigungen

Komponenten und Medien sind initialisiert und programmiert.

Betriebsmeldungen:

Bedeutung	[1]	[1]	Medien
Berechtigt (Öffnen)	1x kurz	1x kurz grün	Benutzer-medien
Unberechtigt (Nicht Öffnen)	4x kurz	4x kurz rot	Benutzer-medien
Berechtigt (Schließen) [3]	1x kurz	1x kurz grün 1x lang rot	Benutzer-medien
Berechtigt (Schließen) [2, 3]	1x kurz 1x lang	—	Benutzer-medien

Legende:

[1] Signale und Anzeigen sind mit der Toolkette (mit der Systemsoftware (z.B. KEM) und dem Programmer) aktivierbar oder deaktivierbar.

[2] Komponenten ohne optische Anzeige.

[3] Schließen mit berechtigten Medien oder betätigen des Tasters (c-lever), wie z. B. für Office Mode, Escape Return und Pass-Mode.

8.3 Berechtigungen Pass-Lock (c-lever)

Bedeutung			Medien
Aktivieren	1x lang	—	Benutzer-medien

Bedeutung			Medien
Deaktivieren (Schliessen)	1x kurz	—	Benutzer-medien
Status (Offen)	—	alle 3 s sehr kurz orange	Benutzer-medien

8.4 Berechtigungen Escape Return und Pass-Mode (c-lever)

Bedeutung			Aktivität
Aktivieren	1x lang	1x sehr lang orange (3 s)	Taster 2 s drücken
Deaktivieren (Schliessen)	1x lang	5x sehr kurz orange	Taster 2 s drücken
Berechtigt (Schliessen)	1x kurz	1x kurz gün 1x lang rot	Benutzer-medien
Status (Offen)	—	1x sehr lang orange (3 s)	Taster kurz drücken
Status (Nicht Offen)	—	5x sehr kurz orange	Taster kurz drücken

8.5 Meldungen bei Anwendung der Sicherheitskarte C2

Beim Anwenden der Sicherheitskarte C2 werden folgende akustische Signale und optische Anzeigen signalisiert.

Hinweis: Die Schreib-Autorisierung wird mit dem INI-Reset gelöscht.

Anwendung der Sicherheitskarte C2:

Ablauf			Medien
Start: Komponente initialisieren	1x kurz	grün, solange sich das Master-Medium im Antennenfeld befindet	Master A oder Master B
Schreib-Autorisierung programmieren.	—	grün, solange der Vorgang nicht beendet ist	Sicherheits-karte C2 15 s im Antennenfeld halten
Ende: Das Programmieren der Schreib-Autorisierung wird beendet	3x kurz	—	—
Löschen der Schreib-Autorisierung der Sicherheitskarte C2	3x kurz	—	—

8.6 Programmiermeldungen

Meldungen beim Programmieren:

Ablauf			Medien
Start: Medien zu programmieren	1x kurz	Die LED leuchtet, wenn sich Medien im Antennenfeld befinden. Sie leuchtet nicht, wenn akustisch signalisiert wird.	Master A und Master B
Bestätigen von programmierten Medien [2]	1x kurz		Master A und Master B
Medium gelöscht [2]	nach 3 s 2x kurz		Benutzer-medien

Ablauf			Medien
Alle Medien gelöscht [2]	nach 10 s [3] 2x kurz		Master B (in A/B Struktur)
	nach 10 s [4] 1x lang 1x kurz		
Ende: Medien zu programmieren	1x lang		Master A und Master B
Fehler beim Programmieren	1x lang	1x kurz rot	
Fehler beim Programmieren [1]	2x lang	—	

Legende:

[1] Komponenten ohne optische Anzeige

[2] Nur für Whitelist-Betrieb ohne Hostsystem

[3] Vor Firmware Version 42

[4] Ab Firmware Version 42

8.7 Wireless

Bedeutung			Tool
Komponente identifizieren [6]	1x kurz	1x lang grün 1x kurz grün	

Legende:

[6] Alle 3 s werden die Signale wiederholt, bis der Vorgang abgeschlossen ist.

8.8 Resetmeldungen

Hinweis: Die Schreib-Autorisierung wird mit dem INI-Reset gelöscht.

Bedeutung			Tool
Bestätigt den Reset	nach 3 s 2x kurz	—	Pinzette INI-Reset Kontakte kurzschließen
Bestätigt den Reset (Whitelist)	nach 10 s 1x lang 1x kurz nach 15 s 2x kurz		Master-Medien
Bestätigt den Reset (CardLink)	nach 15 s 2x kurz		Master-Medien
Bestätigt den Reset	2x kurz		Programmer 1460

8.9 Fehler- und Störungsmeldungen

Bedeutung			Medien
Batterie “Tief” FW 42.XX	1x sehr kurz	9x sehr kurz rot[3]	Benutzermedien Master A und Master B
Batterie “Tief” FW 42.XX[1]	9x sehr kurz[3]	—	Benutzermedien Master A und Master B
Batterie “Leer”	1x sehr lang[3]	—	Benutzermedien Master A und Master B
Selbsttest konnte nicht abgeschlossen werden[5]	8x kurz	8x kurz rot	Benutzermedien
Unberechtigte Medien[4]	4x kurz	4x kurz rot	Benutzermedien
Ausfall der eigenen Uhr in der Komponente[2]	1x lang 1x kurz 1x lang	1x kurz grün	Benutzermedien Master A und Master B
Es konnten nicht alle Sitekeys angelegt werden	1x kurz 1x lang 1x kurz	2x kurz rot	Master A und Master B (MIFARE)
Es konnten nicht alle Schlüssel der Anlage angelegt werden			Servicemedien

Legende:

1 Komponenten ohne optische Anzeige.

2 Bedingung, die Uhr wurde zuvor richtig eingestellt.

3 Anschließend 1x kurz grün und die Komponente öffnet.

4 Batterie "Tief" wird nicht signalisiert.

5 Funktion nur für c-lever, Mechatronikzylinder und Digitalzylinder.
Hinweis: Es wird empfohlen, an den entsprechenden Komponenten eine Zustandskontrolle durchzuführen.

9 Systempflege

9.1 Wartungsplan



ACHTUNG

Gefahr für elektronische Komponenten durch elektrostatische Entladung.

Durch unsachgemäßen Umgang mit elektronischen Leiterplatten oder Komponenten können Schäden entstehen, die zum völligen Ausfall oder zu sporadischen Fehlern führen.

- Bei Installation und Reparatur des Produkts sind die allgemeinen ESD–Schutzmaßnahmen zu beachten.

Nachfolgende Tätigkeiten durchführen, um Schließanlagen und Komponenten über lange Zeit störungsfrei betreiben zu können.

Detaillierte Angaben über Wartungsmaßnahmen befinden sich in den separaten Betriebsanleitungen der jeweiligen Komponenten.



Angaben zu Wartungszeiträumen und Lebenserwartungen von Teilen oder Komponenten können je nach Beanspruchung und Umgebungsbedingungen variieren.
Angegebene Werte beziehen sich auf eine durchschnittliche Beanspruchung.

Prüfen

- Funktionskontrolle der Komponente gemäß Anleitung alle 12 Monate durchführen.
- Prüfen und Einstellen der Uhrzeit mit dem Programmer 1460 alle 12 Monate.
  Im Wireless Betrieb findet die Synchronisation der Uhr über das Wireless Gateway statt.

Update
Firmwareupdate zur Anpassung der Funktionalität jährlich oder nach Bedarf ausführen. Unterschiedliche Firmwarestände der Komponenten einer Anlage vermeiden.

Batterien ersetzen
In den nachfolgenden Tabellen sind die durchschnittlichen Intervalle aufgeführt, nach denen die Batterien der Komponenten ersetzt werden sollten. Die durchschnittliche Lebensdauer ist abhängig vom Batterietyp und den Umgebungsbedingungen. Sie ist auch abhängig von der genutzten Konfiguration (Whitelist / Cardlink), der Ausstattung (standalone / wireless) und den eingestellten Optionen (z.B. akustische Signalisierung).

Batteriestand alle 12 Monate kontrollieren. Batterien gegebenenfalls austauschen.

- Umgebungsbedingungen: Siehe Spezifikationen des Batterieherstellers.
- Batterietyp: Lithium. Nur empfohlene Batterietypen verwenden.

9.2 Batterielebensdauer

Die Lebensdauer einer Batterie als Energiequelle für Standalone-Komponenten ist von vielen Faktoren abhängig.

- Qualitätsschwankungen des Batterieherstellers.
- Art der verwendeten Funktionen einer Komponente.
- Anzahl der verwendeten und/oder kombinierten Funktionen einer Komponente.
- Anzahl der Vorgänge in einer bestimmten Zeitspanne, z. B. pro Tag/Woche/Monat/Jahr.
- Umgebungsbedingungen wie Temperatur, Luftfeuchtigkeit usw.

Die Komponente warnt durch Signale vor niedrigem Batteriestand.

Beispiele für die Batterielebensdauer der verschiedenen Komponenten:

Annahmen für die Tabelle:

- Durchschnittstemperatur 20 °C
- Standalone-Betrieb

- Zutrittsart Whitelist
- Ohne akustische Signalisierung

Komponente	Betätigungen pro Werktag	Intervall
c-lever pro	ca. 250	24 Monate
c-lever		
c-lever compact	ca. 100	24 Monate
Digitalzylinder	ca. 100	12 Monate
	max. 50	24 Monate
Mechatronikzylinder Variante Stulp	ca. 400	12 Monate
	ca. 100	24 Monate
Mechatronikzylinder Varianten - Kompakt - Aufsatz	ca. 50	24 Monate
Schrankschloss 21 10	ca. 100	24 Monate

Batterien in TouchGo Medien:

Komponenten	Batterietyp	Spannung	Art	Temperaturbereich	Lebensdauer
Schlüsselanhänger	CR2450	3 V	Lithium	–20 bis 65 °C	ca. 1 Jahr
Armband	CR2450	3 V	Lithium	–20 bis 65 °C	ca. 1 Jahr
Kartenhalter	CR2430	3 V	Lithium	–20 bis 65 °C	ca. 1 Jahr

9.3 Pufferzeit bei Batteriewechsel

Beim Batteriewechsel ist zu beachten, dass nur eine kurze Zeit für den Wechsel zur Verfügung steht, bevor die Einstellungen der Uhr in den Komponenten verloren gehen (siehe nachfolgende Tabelle).

Hinweis: Einstellungen der Uhr in den Komponenten nach dem Batteriewechsel kontrollieren.

Pufferzeiten:

Komponenten	Pufferzeit
c-lever	< 60 s
c-lever pro	< 45 s
c-lever compact	< 45 s
Digitalzylinder	< 45 s
Mechatronikzylinder • Stulp • Kompakt • Aufsatz	< 45 s
Schrankschloss 21 10	< 120 s

9.4 Öffnung bei entladenen Batterien

Wenn alle Alarmmeldungen bis zur vollständigen Entladung der Batterien ignoriert wurden, können die Komponenten nur noch mithilfe der Notspeisungsfunktion des Programmer 1460 geöffnet werden.

Eine Beschreibung der Notspeisung (Notöffnung) ist in der Bedienungsanleitung des Programmer 1460 zu finden.

Beim Digitalzylinder und beim c-lever compact befinden sich die Batterie(n) im Außenbereich. Nach dem Ersetzen der Batterie(n) die Uhr der Komponente mit dem Programmer 1460 oder über Wireless überprüfen und bei Bedarf einstellen.

Das Schrankschloss 21 10 verfügt nicht über eine Notöffnungsfunktion bei leerer Batterie. Wenn die Batterie leer ist muss das Schloss aufgebrochen werden.

- Die Batterie bei Anzeige "Batterie leer" ersetzen.

9.4.1 Temporäres Notöffnungsmedium

Ein Notöffnungsmedium ist ab FW 42.36 möglich.

Bei leerer Batterie und verlorener Konfiguration kann noch ein temporäres Notöffnungsmedium manuell programmiert werden. Damit kann die Tür einmal geöffnet werden, um den Batteriewechsel vorzunehmen. Die Anwendung des Notöffnungsmediums ist möglich bei

- c-lever
- c-lever pro
- MC-Zylinder

Das Notöffnungsmedium wird mithilfe des Master-Mediums in den RAM-Speicher der Komponente programmiert und ist nur 1 Minute bzw. bis zum nächsten Neustart gültig.

Zur Signalisierung siehe Kapitel Programmiermeldungen [▸ 8.6].

Voraussetzungen

- Batterie tief oder Batterie leer mit Notspeisung
- Das Master-Medium ist vorhanden.
- Das Notöffnungsmedium ist ein Anlagenspezifisches Benutzermedium.
- Betriebsart: Whitelist
- Die Whitelist ist leer.

Vorgehen

1. Das Master-Medium präsentieren.
   ⇨ Signalisierung bei Batterietief: Batterietief, gefolgt von Beginn Programmiermodus
   ⇨ Signalisierung bei Notspeisung: Beginn Programmierung
2. Das als Notöffnungsmedium vorgesehene Benutzermedium präsentieren.
   ⇨ Nur 1 Notöffnungsmedium ist möglich
   ⇨ Das Speichern wird signalisiert.
3. Das Master-Medium präsentieren.

⇨ Nach dem Ende des Programmiervorgangs besteht 1 Minute Zeit, um die Tür mit dem Notöffnungsmedium zu öffnen. Danach ist das Medium wieder aus dem Speicher gelöscht.

9.5 Konfigurationen und Traceback

Die korrekt eingestellten Werte für Datum und Uhrzeit sichern ein aktuelles Zeitmanagement mit den Komponenten.

Komponenten, die über die wireless Funktion mit der Systemsoftware verbunden sind, werden über das Gateway aktualisiert (z. B. Uhrzeit, Konfigurationen). Das Traceback kann mit der Systemsoftware ausgelesen werden.

Bei reinem standalone Betrieb werden die Konfigurationen mit dem Programmer übertragen oder können mit diesem verändert werden (z. B. Uhrzeit einstellen).
Mit einem Programmer kann das Traceback ausgelesen und zur Auswertung an die Systemsoftware übertragen werden.

Weitere Schritte sind in der Bedienungsanleitung des Programmer 1460 beschrieben.

9.6 Firmware-Update von Komponenten

Die Firmware von Komponenten kann im evolo Subsystem aktualisiert werden.

Die neuen Firmware-Versionen werden mit dem Programmer oder über Wireless in die standalone Komponenten übertragen.

Hinweis: Multi RFID (MRD) Komponenten mit manueller Programmierung sind nach einem Firmware-Update auf manuelles Programmieren mit den entsprechenden Medien zu kontrollieren. Bei Bedarf ist ein INI-Reset durchzuführen.

Bei einigen Komponenten (Leser im Online-Betrieb) können Funktionen mit einem Firmware-Update verändert werden.



Falls auf der Komponente Lese-/Schreibberechtigungen vorhanden sind, gilt ab Komponenten-Firmware 42.40 und Programmer-Firmware 01.36 folgendes:
Die Lese-/Schreibberechtigungen (Taufdaten) werden durch das Firmware-Update **nicht** gelöscht.
Falls die Lese-/Schreibberechtigungen gelöscht werden sollen, muss ein INI-Reset durchgeführt werden.

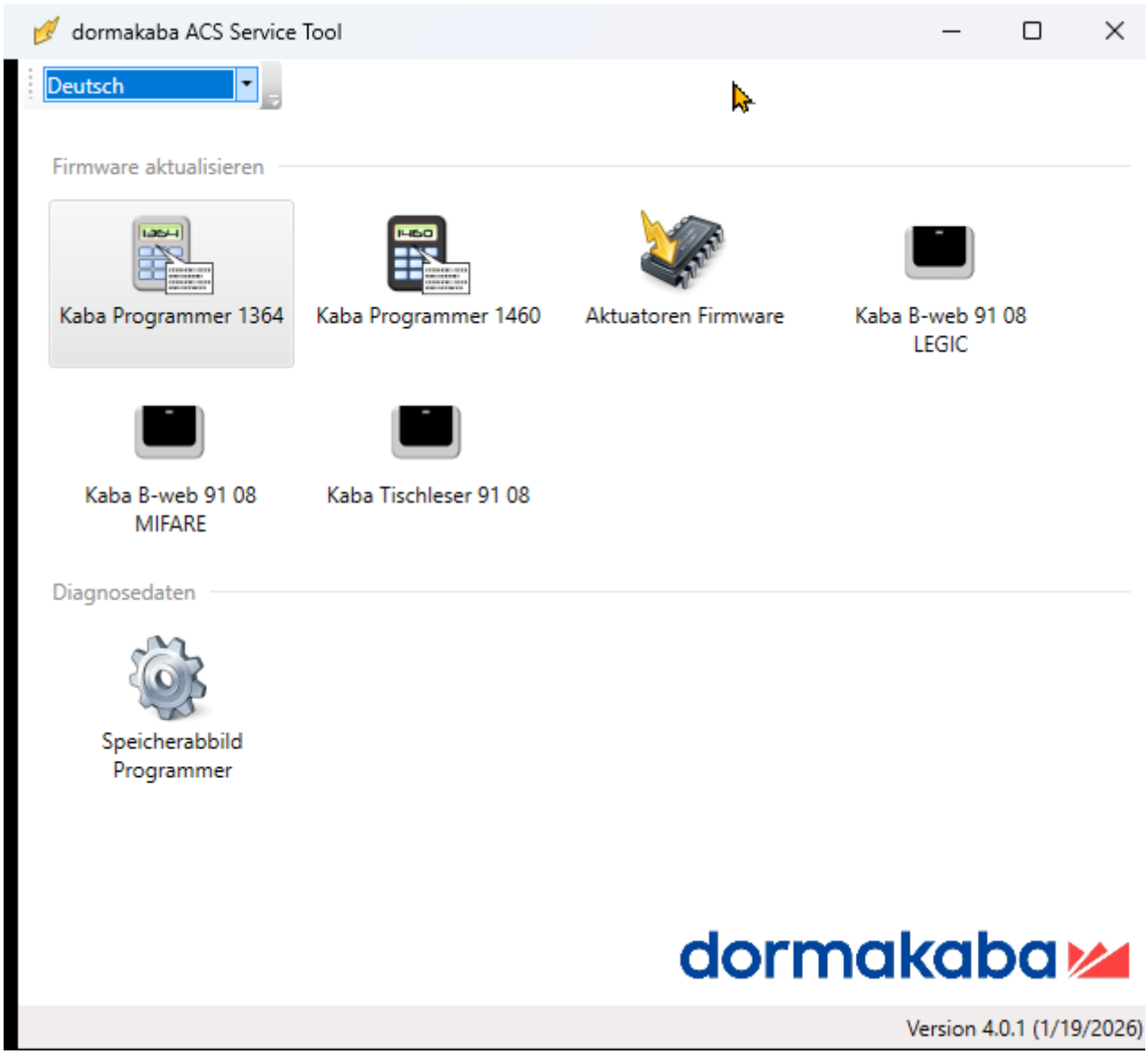
Eine detaillierte Beschreibung ist in der Bedienungsanleitung des Programmer 1460 zu finden.

9.7 dormakaba ACS Service Tool

Das dormakaba ACS Service Tool ist ein Hilfsprogramm zur Aktualisierung von Firmware-Daten und zur Erstellung von Diagnosen.



Das Tool kann auch direkt gestartet werden, d. h., die Systemsoftware muss dazu nicht laufen. Zum Starten *Startmenü -> Programme -> Kaba -> dormakaba ACS Service Tool* aufrufen.



Programmer 1364	Assistent zum Aktualisieren der Programmer-Firmware.
Programmer 1460	Assistent zum Aktualisieren der Programmer-Firmware.
Aktuatoren-Firmware	Assistent zum Übertragen der Firmware für die Komponenten auf den Programmer.
Tischleser 91 08 LEGIC/ MIFARE/MRD	Assistent zum Aktualisieren der Tischleser-Firmware für die gewählte Technologie.
Speicherabbild Programmer 1460	Assistent zum Erstellen einer ZIP-Datei mit dem Speicherinhalt des Programmer. Ein Hilfsmittel zur Problemlösung in Supportfällen.

Die Firmware muss vor dem Aktualisieren aus dem Internet/Extranet auf eine lokale Festplatte heruntergeladen werden.

Der Programmer 1364 ist nicht mehr erhältlich und wird nicht mehr unterstützt. Letzte herunterladbare Firmware: 1.38

www.dormakaba.com

dormakaba Schweiz AG
Mühlebühlstrasse 23
8620 Wetzikon
Schweiz
T: +41 44 931 61 11

www.dormakaba.com