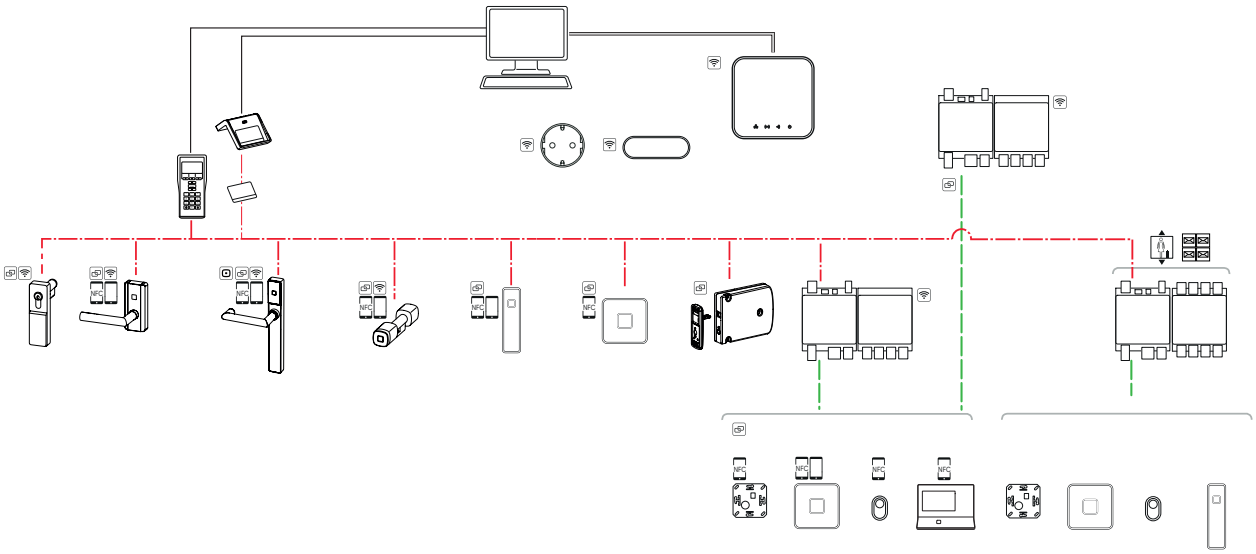
Descrizione del sistema evolo

Descrizione del sistema



Public - 11/2026

IT

Indice

1 Contenuto del documento 5
1.1 Nuove funzioni e aggiornamenti 5
1.2 Validità 5
1.3 Destinatari 5
1.4 Contenuto e obiettivo 6
1.5 Disponibilità dei documenti 6
1.6 Documenti complementari 6
1.7 Abbreviazioni/Definizioni 6
1.8 Avvertimenti 8

2 Panoramica 9
2.1 Autorizzazione 9
2.2 Componenti 9
2.3 Software di sistema 11
2.3.1 Topologie 11
2.3.2 Catena degli strumenti 12
2.4 Opzioni di accesso tramite smartphone 13
2.4.1 Applicazioni Mobile Access 13
2.4.2 Accesso tramite Wallet (Apple Wallet e Google Wallet) 14
2.5 Supporti 14
2.5.1 Supporti master 16
2.5.2 Supporti utente 17
2.6 Strutture di programmazione 18
2.6.1 Struttura A/B e B 18
2.7 Supporto OSS-SO 20

3 Tipi di autorizzazione e funzioni 21
3.1 Numero di identificazione 21
3.2 Livello di sistema 21
3.3 Autorizzazione Whitelist 22
3.3.1 Autorizzazione whitelist con profilo orario 23
3.4 Autorizzazione CardLink 25
3.4.1 Diritti di accesso 25
3.4.2 Convalida 27
3.4.3 Convalida dei supporti 27
3.4.4 Supporti persi 28
3.4.5 Blacklist 29
3.4.6 Supporti di servizio 29
3.4.7 Informazione sullo stato 29
3.4.8 Traceback supporti 29
3.5 Access on Card 29
3.6 Modalità mista 30
3.7 Supporti non autorizzati 30
3.8 Funzioni TimePro 30
3.8.1 Profilo orario Office 30
3.8.2 Profilo orario Day/Night 32
3.9 Funzioni avanzate 32
3.9.1 Componenti wireless 32
3.9.2 Componenti Traceback 35
3.9.3 Modulo S 35
3.9.4 Funzione di rientro (Escape Return) in c-lever pro 35
3.9.5 Modalità Pass per c-lever pro 35
3.9.6 Pass-Lock in c-lever pro 36
3.9.7 Supporti di intervento 36
3.9.8 Disattivazione della programmazione manuale 37
3.10 TouchGo 37
3.10.1 Funzionamento RCID 37
3.10.2 Aspetti di sicurezza 37
3.10.3 TouchGo E110 38
3.10.4 TouchGo E310 38

3.11 Selezione libera dell'armadietto con serratura per armadietti 21 10 e 21 20 39
3.12 Cassetta lettere/ascensore 39

4 Varianti di sistema 40
4.1 Programmazione whitelist 40
4.1.1 Autorizzazione whitelist senza catena degli strumenti 40
4.1.2 Autorizzazione whitelist con catena degli strumenti 41
4.2 Programmazione CardLink 42
4.2.1 Autorizzazione CardLink tramite lettore da tavolo 42
4.2.2 Autorizzazione CardLink tramite lettore di aggiornamento 43
4.2.3 Autorizzazione CardLink tramite terminale 44
4.3 Panoramica delle varianti firmware 45

5 Funzioni di sicurezza 47
5.1 I livelli di sicurezza LEGIC 47
5.2 Sicurezza con le abilitazioni CardLink LEGIC 47
5.3 Sicurezza con l'autorizzazione della whitelist LEGIC 47
5.4 I livelli di sicurezza MIFARE 48
5.5 Sicurezza con le abilitazioni CardLink MIFARE 49
5.6 Sicurezza con l'autorizzazione della whitelist MIFARE 49
5.7 Master T 50

6 Componenti 51
6.1 Dimensioni di memoria 51
6.2 Dati tecnici 51
6.3 Supporti master 54
6.4 Tessere di sicurezza 54
6.5 Catena degli strumenti 55

7 Programmazione / configurazione del componente 57
7.1 Determinazione della tecnologia dei supporti 57
7.2 Metodi di programmazione e configurazione 57
7.3 Programmare i prodotti TouchGo 57
7.3.1 Programmare TouchGo E310 58
7.3.2 Supporti utente persi/guasti 65
7.4 Programmare con i supporti 65
7.4.1 Tessere 66
7.4.2 Chiave 72
7.4.3 Reset INI con supporti master 77
7.5 Programmazione con il software di sistema 79
7.5.1 Software di sistema per componenti evolo 80
7.5.2 Programmazione con software del sistema e Programmer 80
7.5.3 Esportazione in componenti 80
7.5.4 Importazione da componenti 80
7.6 Mobile Access 81
7.6.1 Requisiti di sistema 81
7.6.2 Inizializzazione del dispositivo per il Mobile Access 82
7.6.3 Inizializzazione del dispositivo per evolo smart 83
7.6.4 Regolazione della potenza del segnale Bluetooth 83
7.7 Inizializzazione di componenti wireless 83
7.8 Impostare proprietà e funzioni di un componente 84
7.9 Reset (reset INI) 84
7.9.1 Panoramica delle varianti di reset INI dei componenti 85
7.10 Risparmio energetico 85
7.10.1 Disattivare funzioni 86
7.10.2 Funzione Object in Field 87

8 Segnali 88
8.1 Durata del segnale 88
8.2 Autorizzazioni d'accesso 88
8.3 Autorizzazioni Pass-Lock (c-lever) 88
8.4 Autorizzazioni Modalità Escape-Return e Pass (c-lever) 89
8.5 Segnalazioni di applicazione della tessera di sicurezza C2 89

8.6 Segnalazioni di programmazione 89
8.7 Wireless 90
8.8 Segnalazioni di reset 91
8.9 Messaggi di errore e di guasto 92

9 Manutenzione del sistema 93
9.1 Piano di manutenzione 93
9.2 Durata delle batterie 93
9.3 Tempo tampone nella sostituzione della batteria 94
9.4 Apertura a batterie scariche 94
9.4.1 Supporto temporaneo di apertura di emergenza 95
9.5 Configurazioni e Traceback 95
9.6 Aggiornamento firmware dei componenti 96
9.7 dormakaba ACS Service Tool 96

1 Contenuto del documento

1.1 Nuove funzioni e aggiornamenti

La tabella seguente contiene i miglioramenti apportati in questa versione del sottosistema, dei componenti associati o del software/firmware.

Modifica	Descrizione	Intro-dotta in
Ritardo di attivazione del Pass-Lock	È possibile impostare un ritardo configurabile per evitare l'attivazione involontaria del Pass-Lock. Per attivare il Pass-lock, il tasto deve essere tenuto premuto per l'intera durata configurata. Si veda il capitolo Pass-Lock in c-lever pro [▶ 3.9.6].	42.48
Supporti di intervento	È possibile definire un gruppo dedicato di supporti di intervento per mantenere l'accesso quando il Pass-Lock è attivo o quando un sistema di rilevamento delle intrusioni (IDS) è attivato. Vedi Supporti di intervento [▶ 3.9.7].	42.48
Supporta Google Wallet	Google Wallet può essere utilizzato come supporto utente tramite NFC sui componenti evolo supportati. Si veda il capitolo Accesso tramite Wallet (Apple Wallet e Google Wallet) [▶ 2.4.2].	42.48
Supporta Apple Wallet	Apple Wallet può essere utilizzato come supporto utente tramite NFC sui componenti evolo supportati. Si veda il capitolo Accesso tramite Wallet (Apple Wallet e Google Wallet) [▶ 2.4.2].	42.46
Opzione Access on Card (AoC) per una validità illimitata	Quando si utilizza MATRIX, è possibile impostare una validità di accesso illimitata per un utente, se ciò è richiesto dalle esigenze aziendali del cliente. Si veda il capitolo Access on Card [▶ 3.5].	42.40
Aggiornamento della designazione del wireless gateway	Per tenere conto degli ultimi miglioramenti, questo manuale descrive il wireless gateway nella sua versione attuale **90 40-K7**.	-
c-lever air interrotto	Il prodotto non è più offerto ai clienti e non è più menzionato in questo manuale.	-

1.2 Validità

Il presente documento descrive il sottosistema evolo per le tecnologie RFID LEGIC, MIFARE e MRD (Multi RFID Device). Nei nuovi impianti si utilizza la tecnologia MRD.

Il documento descrive il sottosistema evolo per l'utilizzo delle tecnologie mobili Bluetooth® e NFC.

La descrizione comprende componenti standalone, wireless, Bluetooth® e NFC.

Versione del firmware installato sui componenti: dalla versione 42.38

Le descrizioni e gli esempi sull'impiego dei componenti con i sistemi host nel presente manuale si riferiscono all'impiego con KEM. L'integrazione del sottosistema evolo nei sistemi host è descritta nelle documentazioni dei rispettivi sistemi host.

1.3 Destinatari

La presente documentazione è rivolta esclusivamente al personale specializzato.

Le descrizioni presuppongono la presenza di personale specializzato formato dal produttore. Le descrizioni non sono da intendersi come sostitutive dei corsi di formazione sul prodotto.

Per motivi di sicurezza degli strumenti gli interventi di installazione, manutenzione e riparazione descritti nel presente documento possono essere eseguiti soltanto da addetti specializzati abilitati secondo la normativa EN 62368-1 (Apparecchiature per tecnologie di comunicazione, informazione e audio/video Requisiti di sicurezza - Parte 1).

"Personale tecnico specializzato" è il termine che indica le persone con un'adeguata istruzione tecnica ed esperienza con la tecnologia della struttura. Il personale tecnico specializzato è tenuto ad applicare la propria formazione ed esperienza per identificare e ridurre al minimo i pericoli per se stessi e per gli altri durante l'esecuzione delle attività. È responsabilità del personale tecnico specializzato garantire che le condizioni specificate dal produttore, nonché le normative e gli standard applicabili siano rispettati durante l'utilizzo del prodotto descritto.

La presente documentazione serve inoltre a informare le persone a cui sono assegnate le seguenti mansioni:

- Pianificazione e realizzazione del progetto
- Messa in funzione del prodotto all'interno dell'ID modello
- Collegamento del prodotto al software applicativo tramite la programmazione di applicazioni per clienti
- Adattamento personalizzato tramite la parametrizzazione del prodotto

1.4 Contenuto e obiettivo

Il presente documento contiene le informazioni di base del sistema evolo fornendo una panoramica sintetica.

1.5 Disponibilità dei documenti

Ulteriore documentazione è disponibile al seguente link:

https://techdoc.dormakaba.com/cds

1.6 Documenti complementari

I seguenti documenti sono disponibili presso i partner commerciali:

- Documentazione tecnica dei componenti utilizzati
- Manuale Programmer 1460
- Documentazione del software di sistema utilizzato
- Catalogo dei prodotti dormakaba evolo

Opzione TouchGo

- Istruzioni per l'uso di dormakaba c-lever pro TouchGo
- Linea guida di pianificazione dormakaba c-lever pro TouchGo con modulo S

Opzione wireless

- Direttiva di progettazione wireless

Opzione Mobile Access

- Linee guida per la pianificazione Mobile Access

1.7 Abbreviazioni/Definizioni

Per facilitare la lettura, le seguenti denominazioni ufficiali dei prodotti vengono sostituite da denominazioni abbreviate.

Denominazione prodotto/Definizione	Denominazione abbreviata
dormakaba evolo	evolo

Denominazione prodotto/Definizione	Denominazione abbreviata
Lettore remoto dormakaba	Lettore
Lettore compatto dormakaba	
Cilindro digitale dormakaba	Cilindro digitale
Cilindro meccatronico ad applicazione dormakaba	Cilindro meccatronico
Cilindro meccatronico compatto dormakaba	
Cilindro meccatronico con risvolto dormakaba	
Terminale dormakaba 94 20	Terminale
dormakaba c-lever pro TouchGo	TouchGo
dormakaba c-lever pro	c-lever
dormakaba c-lever compact	
Kaba c-lever	
Serratura per armadietti dormakaba 21 10	Serratura per armadietti
Wireless Gateway 90 40-K7	Wireless gateway
Wireless Extender 90 41	Extender
Lettore remoto dormakaba 91 15 (E320) con modulo d'ampliamento wireless 90 43	Wireless Reader
Lettore da tavolo dormakaba 91 08	Lettore da tavolo
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
Numero unico	UID
Numero di identificazione della tessera	CID
Identificazione a radiofrequenza	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

I seguenti simboli rappresentano segnali acustici o ottici:

Simboli		Tipo di segnale
		Segnale acustico
		Segnale ottico

Nei componenti senza possibilità di visualizzazione ottica non è possibile alcuna segnalazione ottica.

1.8 Avvertimenti

Il presente manuale contiene avvertimenti che devono essere osservati per la propria sicurezza personale e per evitare danni materiali. Gli avvertimenti relativi alla sicurezza personale sono evidenziati da un triangolo di avvertenza, mentre gli avvertimenti riferiti solamente ai danni materiali vengono riportati senza questo triangolo. A seconda del livello di pericolo, gli avvertimenti vengono visualizzati in ordine decrescente come segue:



⚠ PERICOLO

Rischio alto

Indica un pericolo imminente che potrebbe causare gravi lesioni fisiche o la morte.



⚠ AVVERTENZA

Rischio medio

Indica una situazione potenzialmente pericolosa che potrebbe causare gravi lesioni fisiche o la morte.



⚠ ATTENZIONE

Rischio basso

Indica una situazione potenzialmente pericolosa che potrebbe causare lesioni fisiche lievi.



AVVISO

Informazioni importanti sull'uso corretto del prodotto

Il mancato rispetto di queste istruzioni potrebbe causare malfunzionamenti. Il prodotto potrebbe venire danneggiato.

Se sono presenti contemporaneamente diversi livelli di pericolo, viene sempre utilizzato l'avvertimento del livello più alto. Se un avvertimento mette in guardia dal pericolo di lesioni personali, lo stesso avvertimento può anche indicare pericolo di danni materiali.

Altri simboli di pericolo:



Pericolo generale



Pericolo di esplosione



Pericolo dovuto alla tensione elettrica



ESD: pericolo dovuto a scariche elettrostatiche

Gli avvertimenti e le informazioni utili per il funzionamento sicuro del prodotto sono contrassegnati come segue:



Consigli per l'applicazione, informazioni utili.
Aiutano a ottimizzare l'utilizzo del prodotto e delle relative funzioni.

2 Panoramica

Il sottosistema evolo è un insieme di componenti standalone la cui configurazione viene trasmessa per mezzo della toolchain.

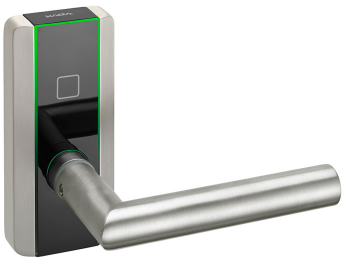
2.1 Autorizzazione

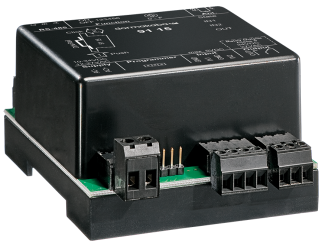
Descrizione

Autorizzazione	Descrizione
Whitelist	Le informazioni relative all'autorizzazione si trovano nei componenti.
CardLink	Le informazioni relative all'autorizzazione si trovano nei supporti utente.
Access on Card AoC	Utilizzato solo con MATRIX: Le informazioni relative all'autorizzazione si trovano nei supporti utente. Ulteriori informazioni su AoC sono disponibili nella documentazione MATRIX.
OSS-SO	Standard aperto. Ulteriori informazioni si trovano qui: http://www.oss-association.com/standards/oss-standard-offline/
Mobile Access	Con Mobile Access lo smartphone si trasforma in supporto utente.

2.2 Componenti

Componenti elettronici con varie funzioni, che possono essere installati nelle o sulle porte.

	Panoramica del sistema Componenti	
Numero prodotto	**Componente**	**Descrizione**
		c-lever pro **Opzioni:** • Wireless • Mobile Access • OSS-SO • TouchGo E110 solo standalone, non per sottosistemi evolo wireless non disponibile • TouchGo E310 per sottosistemi evolo wireless non disponibile
		c-lever compact **Opzioni:** • Wireless • Mobile Access • OSS-SO

	Panoramica del sistema Componenti	
Numero prodotto	**Componente**	**Descrizione**
143x / 153x		Cilindro digitale **Opzioni:** • Wireless • Mobile Access • OSS-SO
21 20		Serratura per armadietti • OSS-SO
91 15	 	Lettore remoto Dispositivo con unità di rilevamento separata **Opzioni aggiuntive:** • Wireless se utilizzato con il modulo d'ampliamento 90 43 (non raffigurato) • Mobile Access (Bluetooth con relativa unità di rilevamento) • OSS-SO • Abbinato al sottoterminale per lettore compatto dormakaba 91 10

	Panoramica del sistema Componenti	
Numero prodotto	**Componente**	**Descrizione**
91 04	 	Lettore compatto **Opzioni:** • Mobile Access solo NFC NFC e Bluetooth • OSS-SO • Abbinato al sottoterminale per lettore compatto dormakaba 91 10
		Cilindro meccatronico **Opzioni:** • Wireless • OSS-SO
		Soluzione per accesso cassette lettere/comando ascensore • Mobile Access

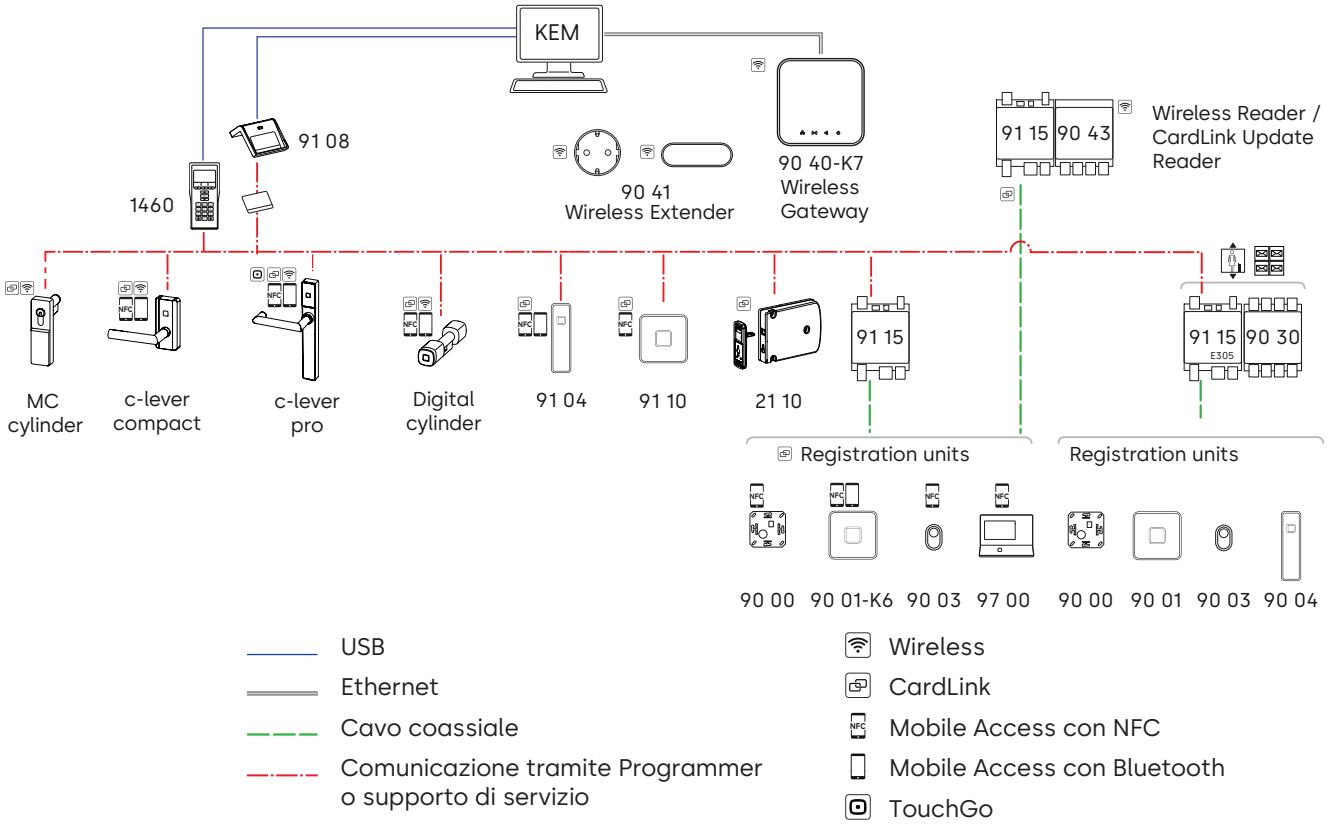
2.3 Software di sistema

È possibile configurare i componenti evolo, oltre che con il dormakaba evolo Manager (KEM), anche con un altro software di sistema.
Le informazioni sulle possibilità sono descritte nella documentazione del software di sistema utilizzato.

2.3.1 Topologie

Un esempio di una possibile topologia.

Componenti evolo con KEM:
Edizione: 03/2026



Legenda			
90 00 90 01 90 03 90 04	Unità di rilevamento (Registration unit)	91 04 91 10	Lettore compatto
90 40-K7	Wireless gateway	91 15 91 25	Lettore remoto
90 41	Wireless Extender	90 30 90 43	Modulo d'ampliamento
1460	Programmer	91 08	Lettore da tavolo B-web
91 15 + 90 30	Comando ascensore/cassetta delle lettere	91 15 + 90 43	Lettore wireless Lettore di aggiornamento CardLink wireless

Le linee guida di pianificazione per wireless e Mobile Access comprendono altre informazioni su questi argomenti.

Mobile Access con NFC: Mobile Access deve essere abilitato nel componente.
Mobile Access con Bluetooth: Il componente dispone dell'hardware necessario per Bluetooth e Mobile Access è abilitato nel componente.

Si veda anche il capitolo [▸ 2.4.1]

2.3.2 Catena degli strumenti

Software di sistema e hardware per la gestione, la lettura e la scrittura dell'autorizzazione nei componenti e nei supporti.

Panoramica del sistema Catena degli strumenti	
Strumento	**Descrizione**
	Lettore da tavolo 91 08 MRD Tramite il software di sistema e il lettore da tavolo i supporti vengono letti e scritti.
	Programmer 1460 Il dispositivo funge da anello di congiunzione tra i componenti standalone e il software di sistema. Il dispositivo viene utilizzato anche per la prima configurazione/il collegamento dei componenti wireless a una rete wireless.
	Wireless Gateway 90 40-K7 Il dispositivo consente il collegamento dei componenti wireless al software di sistema.
	Wireless Extender 90 41 Il dispositivo aumenta la portata del wireless gateway.
	Wireless Reader Collegamento wireless per il lettore remoto 91 15 tramite un modulo d'ampliamento wireless 90 32 inserito. Per l'aggiornamento CardLink tramite wireless.
	Terminale Per l'aggiornamento CardLink

2.4 Opzioni di accesso tramite smartphone

In alternativa ai consueti supporti di accesso, gli utenti possono utilizzare applicazioni mobili o l'accesso tramite Wallet. Per i dettagli, si vedano i capitoli seguenti.

2.4.1 Applicazioni Mobile Access

Nelle applicazioni Mobile Access, l'accesso avviene sfruttando le funzionalità di uno smartphone. Con l'autorizzazione all'accesso la serratura/porta può essere aperta manualmente. Quando l'accesso viene concesso, l'utente viene informato tramite un segnale ottico e acustico.

La configurazione è possibile parallelamente all'accesso convenzionale con i supporti.

Requisiti tecnici per utilizzare le funzionalità complete:

Per poter utilizzare Bluetooth, il componente deve essere provvisto dell'hardware corrispondente.

- Verificare le funzionalità Bluetooth del componente per mezzo del Programmer.

Tecnologia	Smartphone Sistema operativo	Componente
NFC	Android	Dotazione standard e Mobile Access abilitato
NFC + BLE	Android iOS	Hardware con funzionalità Bluetooth e Mobile Access abilitato

App	Descrizione
App mobile access	App per smartphone per l'apertura delle porte. Supporto utente
VCP Installer	App per smartphone per la messa in servizio di componenti porta (componenti evolo, lettori accessi).
evolo smart	App per smartphone per la messa in servizio e la gestione di componenti porta. Software di sistema.

Software di sistema

Il software di sistema [▶ 2.3] serve a gestire il piano di chiusura. Nelle versioni attuali, Mobile Access può essere configurato nel piano di chiusura. Si veda il capitolo Requisiti di sistema [▶ 7.6.1].

2.4.2 Accesso tramite Wallet (Apple Wallet e Google Wallet)

Apple Wallet e Google Wallet possono essere utilizzati come supporti utente sui componenti evolo supportati. L'accesso viene concesso all'utente tramite NFC avvicinando lo smartphone al componente. Per questa funzione non è necessaria l'app dormakaba.

L'accesso tramite Wallet è indipendente dal Mobile Access basato su Bluetooth. Non è richiesta alcuna licenza Mobile Access aggiuntiva; sono pertanto sufficienti i componenti delle linee di prodotti E300 ed E320.

Requisiti e limitazioni

- Il firmware del componente deve essere della versione 42.46 o superiore (Apple Wallet) oppure 42.48 o superiore (Google Wallet).
- Se nello stesso impianto vengono utilizzati supporti MIFARE, è necessario MIFARE DESFire. Le credenziali Wallet non sono compatibili con MIFARE Classic.
- È necessario il supporto da parte del sistema host. Si veda la documentazione di configurazione del rispettivo sistema host.

2.5 Supporti

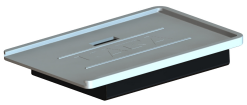
I supporti master non dispongono di autorizzazioni di accesso.

Panoramica del sistema Supporti	
Supporto	**Descrizione**
Supporti master	
	Scheda Master A Cilindro meccatronico master A chiave
	Scheda master B Cilindro meccatronico master B chiave

Panoramica del sistema Supporti	
Supporto	**Descrizione**
	Scheda master T (impiego solo con KEM)
	TouchGo supporto master (RCID, solo TouchGo E110)

Con la loro autorizzazione di accesso programmata, i supporti utente vengono utilizzati in porte e gruppi porte.

Panoramica del sistema Supporti	
Supporto	**Descrizione**
Supporti utente	
	Scheda
	Scheda con codice QR (evolo smart)
	Cilindro meccatronico
	Portachiavi
	Portachiavi con codice QR (evolo smart)
	Mobile Access L'autorizzazione d'accesso avviene tramite smartphone. In varie applicazioni anche la configurazione dei componenti è possibile tramite smartphone. Si veda il capitolo LINK [▶ 2.4.1]: Applicazioni Mobile Access
	Portachiavi TouchGo

Panoramica del sistema Supporti	
Supporto	**Descrizione**
	Braccialetto TouchGo
	Porta-scheda TouchGo

Supporti speciali:

Panoramica del sistema Supporti	
Supporto	**Descrizione**
Tessere di sicurezza	
	La tessera di sicurezza viene creata per ciascun impianto di chiusura e consente la sicurezza dell'impianto. • MIFARE: Tessera di sicurezza C • LEGIC: Tessera di sicurezza C1 e C2
Supporto di prova wireless	
	Consente, ad es., la misurazione del raggio d'azione per i componenti wireless. Solo per componenti wireless. Ulteriori informazioni si trovano nella linea guida di pianificazione wireless.
Schede di licenza	
	Upgrade livello di sistema Ulteriori informazioni si trovano nel capitolo Livello di sistema Capitolo [▶ 3.2].

2.5.1 Supporti master

Con i supporti master, nei componenti standalone viene avviato o terminato il procedimento di programmazione.

Senza sistema host:

- Dopo aver avviato la procedura, viene configurata una whitelist manuale.
  Si veda il capitolo "Programmazione con supporti"
- I master B vengono gestiti con un master A. Le informazioni sulle strutture di programmazione si trovano nel capitolo "Strutture di programmazione"
- I supporti master non dispongono di autorizzazione di accesso.

Con sistema host:

La documentazione del sistema host impiegato contiene informazioni sull'impiego dei supporti master.

- Dopo aver avviato la procedura, per mezzo del Programmer viene caricato un file di programmazione.
  Si veda "Programmazione con il software di sistema".

Componenti wireless:

- È necessario un supporto master per stabilire la connessione del componente con il wireless gateway per mezzo del Programmer.

Master T:
I master T sono master temporanei dalla validità e funzionalità limitate. I master T non sono possibili in tutti i sistemi host. Si veda la documentazione del sistema host impiegato.

TouchGo:
Il TouchGo E110 è programmabile solo con whitelist standalone e non può essere utilizzato con un sistema host. Per la programmazione è richiesto il master RCID.

Il TouchGo E310 può essere impiegato solo in un sottosistema evolo con sistema host e toolchain. Le autorizzazioni RCID e RFID vengono configurate nel software di sistema e connesse al componente tramite accoppiamento. Viene utilizzato il supporto master valido per il sottosistema evolo.

Supporti



TouchGo



RCID solo TouchGo E110

2.5.2 Supporti utente

Con i supporti utente, si consente agli utenti di esercitare le autorizzazioni d'accesso loro assegnate, ad es. aprendo le porte.

Senza sistema host
Nella programmazione whitelist i supporti utente vengono raggruppati in un master B.

AVVISO

Accesso non autorizzato con supporto perso

Rimuovere il supporto perso dai componenti:

- Utilizzare il Master per annullare tutte le autorizzazioni di accesso (rimuovere dalla whitelist), vedere il capitolo "Annulla tutte le autorizzazioni di accesso assegnate dal Master B".
- Assegnare le autorizzazioni di accesso ai supporti utente ancora validi (inserire nella whitelist), vedere il capitolo "Assegna le autorizzazioni di accesso".
- Ripetere la procedura su tutti i componenti a cui ha accesso il supporto perso.

Con sistema host

Le autorizzazioni di accesso dei supporti utente vengono programmate per mezzo dei file di configurazione. Maggiori informazioni in merito si trovano nel capitolo "Programmazione con il software di sistema" [▶ 7.5.2].

Supporti

RFID





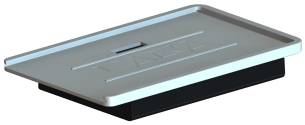


NFC/Bluetooth



TouchGo







Supporto utente	RCID
Supporto combinato	RCID + RFID

2.6 Strutture di programmazione

Solo in caso di programmazione standalone senza sistema host.
Solo programmazione whitelist.

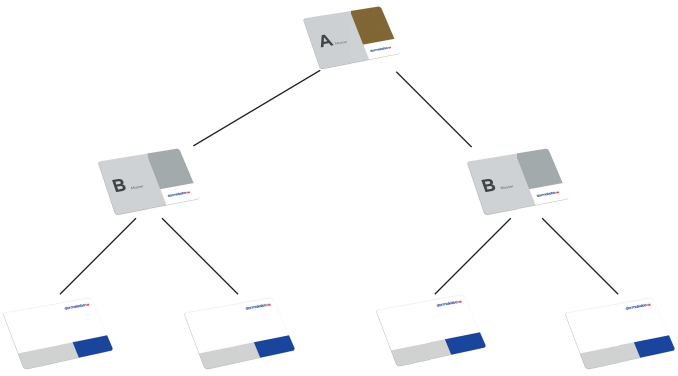
Organizzazione dei componenti in una struttura A/B o B.

La programmazione viene descritta nel capitolo "Programmazione con supporti".

2.6.1 Struttura A/B e B

Sistemi basati su tessera:

Struttura A/B

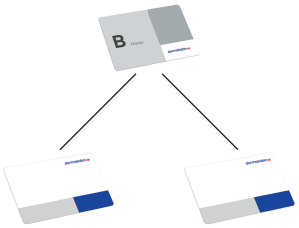


Master-A

Master-B

Supporti utente

Struttura B

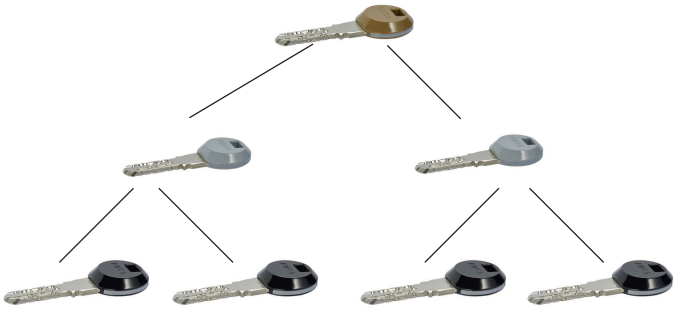


Master-B

Supporti utente

Sistemi meccatronici:

Struttura A/B

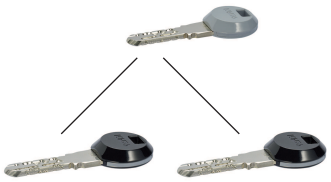


Master-A

Master-B

Supporti utente

Struttura B



Master-B

Supporti utente

Descrizione/Esempi
Struttura A/B:

Master-A:

- Creazione di un massimo di 200 master
- Nessuna programmazione dei supporti utente
- Nessuna programmazione di autorizzazioni d'accesso
- Per ulteriori applicazioni vedere il capitolo seguente

Master-B:

- Assegnazione e revoca di autorizzazioni di accesso

Supporti utente:

- Massimo 4000 supporti utente
- L'assegnazione dei diversi master B agli utenti è arbitraria

Esempio per 1 componente di un impianto

- Master B1: 50 utenti
- Master B2: 3950 utenti

Totale = 4000: Il numero massimo di utenti è stato raggiunto.

Struttura B:

Master-B:

- Assegnazione e revoca di autorizzazioni di accesso
- Per ulteriori applicazioni vedere il capitolo seguente

Supporti utente:

- Massimo 4000 supporti utente

- **Non** è possibile assegnare agli utenti più di un master B.

Esempio per 1 componente di un impianto

- Master-B: 4000 utenti

Totale = 4000: Il numero massimo di utenti è stato raggiunto.

2.7 Supporto OSS-SO

OSS-SO (Open Security Standards – Standard Offline) è uno standard industriale aperto per il controllo accessi offline basato su tessera. Consente l'interoperabilità tra sistemi di controllo accessi e dispositivi di chiusura offline di produttori diversi. Le autorizzazioni di accesso vengono salvate sul supporto utente (Data on Card) e lette direttamente dal componente. Il componente non deve essere collegato al sistema host.

I componenti evolo possono essere utilizzati con OSS-SO. La configurazione avviene tramite la catena degli strumenti OSS-SO e i file XML forniti dal sistema host.

Limitazioni
Le seguenti funzioni non sono supportate in caso di funzionamento con OSS-SO:

- Funzioni di commutazione del modulo S Modulo S [▶ 3.9.3]
- Modalità Pass Modalità Pass per c-lever pro [▶ 3.9.5]
- Pass-Lock Pass-Lock in c-lever pro [▶ 3.9.6]

Comportamento del cilindro meccatronico in modalità Office con OSS-SO
La modalità Office non è supportata dal cilindro meccatronico. Se il cilindro fa parte di un gruppo di accesso per il quale sono configurate autorizzazioni di commutazione (toggle) OSS-SO, il componente esegue un'apertura normale invece di attivare la modalità Office. Questo comportamento corrisponde a quello del funzionamento con CardLink.

Ulteriori informazioni su OSS-SO:

- http://www.oss-association.com/standards/oss-standard-offline/
- Manuale di riferimento file XML OSS-SO
- Istruzioni per l'uso della catena degli strumenti OSS-SO

3 Tipi di autorizzazione e funzioni

Il capitolo descrive i due tipi di autorizzazione Whitelist e CardLink e le rispettive funzioni dei componenti evolo corrispondenti.

- Whitelist: Si veda il capitolo
- CardLink: Si veda il capitolo
- AoC: Si veda il capitolo [▶ 3.5]

3.1 Numero di identificazione

Ai supporti e ai componenti viene assegnato un numero di identificazione per l'autorizzazione. Questo consente un'identificazione univoca.

Il numero unico (UID) è un numero di identificazione univoco, assegnato dal costruttore di schede e salvato nei supporti utente. senza poter essere modificato oppure cancellato.

Il Card ID (CID) è un numero di identificazione univoco, assegnabile tramite il software di sistema. Attualmente ciò è possibile solo con KEM. È possibile ordinare supporti con CID definito. Il CID è salvato nel supporto utente con la chiave impianto unica e viene letto dai componenti dell'impianto.

3.2 Livello di sistema

I componenti sono consegnati al cliente con un livello di sistema preimpostato. Il livello di sistema impostato determina la compatibilità del componente con il sistema host impiegato. I sistemi host consentono la configurazione per il livello di sistema loro assegnato. Un componente con un livello di sistema inferiore non può essere configurato. Un componente con un livello di sistema superiore può essere utilizzato su un sistema host con un livello di sistema inferiore.

Panoramica
Panoramica dei sistemi host utilizzati e del livello di sistema corrispondente.

Sistema	Livello di sistema	Definizione sul programmer
		Firmware a partire da 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

Il livello di sistema di un componente può essere determinato con l'aiuto del Programmer.

Rilevare lo stato livello di sistema e “BLE ready”.
Selezionare sul programmer il menu 'Info attuatore' e leggere le informazioni provenienti dal componente.

Requisiti preliminari:

- Programmer 1460
- Supporto master del componente

Procedura:

1. Registrarsi nel sistema del componente tramite supporto master.
2. Selezionare il menu leggi l'attuatore.
3. Selezionare la voce del menu 'Info'.
4. Connettere il programmer con il componente.

Rilevare la variante del firmware (E3xx) e la versione.

Con SL si indica il livello di sistema (system level).

Per BLE la spunta indica che BLE è attivo.

Il livello di sistema viene supportato a partire dalle seguenti versioni dei componenti e sistemi host.

Ora il componente può essere configurato, a condizione che il livello di sistema del componente e il file di configurazione corrispondano.

Il componente può essere configurato se il livello di sistema del componente è più grande del livello di sistema del sistema host (Ciò si applica da SL1 fino a SL3. Non vale per SL4).

Un aggiornamento del firmware è possibile anche con un livello di sistema errato.

Sistema host	a partire dalla versione	Note
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	Il programmer confronta il livello di sistema del file parametri con il livello di sistema del componente.
Componente (versione firmware)	42.28	In fabbrica viene impostato un livello di sistema in seguito all'ordine.

Upgrade ad un livello di sistema superiore

I componenti vengono consegnati dalla fabbrica con il livello di sistema ordinato. Quando occorre utilizzare funzioni che non sono abilitate nel dato livello di sistema, quest'ultimo deve allora essere portato sul componente allo stato necessario. A tal fine, possono essere acquistati dei supporti di upgrade.



Sono disponibili i seguenti supporti per upgrade/licenza successiva:

Upgrade	da SL1 a SL2
Upgrade	da SL2 a SL3
Upgrade	da SL1 a SL3
Licenza	Mobile Access tramite BLE

La procedura di upgrade è descritta nel manuale tecnico del componente.

3.3 Autorizzazione Whitelist

Un'autorizzazione Whitelist è costituita dalla quantità di supporti autorizzati registrati nel componente.

L'autorizzazione Whitelist viene programmata nei componenti.
In altre parole, l'UID o il Card ID (CID) dei supporti da autorizzare viene memorizzato nei componenti e quindi registrato nella Whitelist.
Nella Whitelist viene confrontato l'UID o il CID dei supporti presentati. Se c'è concordanza, i supporti sono autorizzati e i componenti si aprono. La Whitelist può contenere fino a 4.000 voci. È possibile registrare l'UID o il CID.

Esempio funzionale

L'autorizzazione di accesso viene concessa solo se vengono presentati supporti utente il cui UID o CID è memorizzato nei componenti.

Componenti	Supporti	Accesso
Lista dell'UID memorizzato nei componenti	**UID dei supporti presentati**	
570AE209	570AE209	✓
222BE121	222BE121	✓
—	878EAE964	✗
—	121AC001	✗

3.3.1 Autorizzazione whitelist con profilo orario

I profili orari vengono utilizzati per definire gli orari in cui i supporti sono autorizzati per i componenti.

Tutti i componenti di evolo hanno un proprio orologio (Real Time Clock). In questo modo è possibile concedere all'utente un'autorizzazione di accesso ai supporti basata sul tempo per ogni componente e porta.

Oltre all'autorizzazione di accesso di base, i profili orari possono essere utilizzati per limitare la durata di un'autorizzazione. I profili orari sono definiti nel software del sistema.

3.3.1.1 Autorizzazione whitelist con profilo orario individuale

Per ciascun componente sono disponibili in tutto15 profili orari definibili liberamente con 12 finestre orarie.

3.3.1.2 Autorizzazione whitelist con profilo orario "Sempre" non modificabile

Questo profilo orario ha lo stato "Sempre" e garantisce l'apertura 24 ore al giorno, 7 giorni alla settimana. Il profilo orario "Sempre" non può essere modificato, rinominato o cancellato.

3.3.1.3 Ferie/Giorni particolari

Giorni particolari disponibili:

Profilo orario V4	Dispone di due giorni particolari A e B

Nota: Se i componenti sono aggiornati con il Programmer 1460, il software di sistema acquisisce sempre i giorni festivi e particolari attuali (dello stesso giorno o futuri).

Profili orari per ferie

Per i periodi comprendenti diversi giorni consecutivi (ad esempio i periodi di ferie) è possibile accordare o negare l'autorizzazione di accesso. Per stabilire la durata di un periodo, immettere una data di inizio e una data di fine. È possibile impostare vari blocchi di ferie. Nei componenti (V4) possono essere definiti in tutto 20 blocchi di ferie.

Nota sulla rappresentazione dei giorni particolari all'interno di blocchi di ferie: Se i giorni particolari sono all'interno di un blocco di ferie, saranno privilegiati nella rappresentazione, nel senso che la rappresentazione del giorno particolare si sovrappone a quella del blocco di ferie. Se si elimina il giorno particolare, il blocco di ferie sarà visualizzato completamente.

Finestra oraria dedicata a giorni particolari

Per quanto riguarda i giorni particolari (ad es. i giorni eccezionali), è possibile creare rispettivamente 2 giorni diversi, il giorno particolare A e il giorno particolare B. In questo modo possono essere create due finestre orarie, ad esempio una per la vigilia di un giorno eccezionale (giorno particolare A) e una per il giorno eccezionale stesso (giorno particolare B). Per ognuna delle 2 tipologie, nei componenti possono essere impostati fino a 32 giorni particolari.

Tipologie di giorni particolari	Giorno particolare	Max Numero di giorni particolari nel componente
Giorno particolare A	Vigilia di un giorno eccezionale	32
Giorno particolare B	Giorno eccezionale	32

3.3.1.4 Ora legale/solare

Nei componenti, il cambio di orario legale/solare avviene automaticamente in base al fuso orario mondiale impostato, a seconda del software di sistema utilizzato.

3.4 Autorizzazione CardLink

Per la tipologia di autorizzazione CardLink, l'autorizzazione di accesso viene gestita dai supporti utente, senza la necessità di eseguire interventi di gestione locali sui componenti. Per questa tipologia di autorizzazione sono necessarie le applicazioni supporti sui supporti utente. Al momento della messa in funzione, i componenti devono essere programmati una sola volta.

Questa tipologia di autorizzazione consente anche la convalida (attivazione per un tempo determinato – Convalida [▶ 3.4.2]) dei supporti utente per l'autorizzazione di accesso nei componenti standalone.

Vantaggi

- L'autorizzazione di accesso viene scritta direttamente nei supporti utente.
- L'autorizzazione può essere limitata temporalmente nella funzione **Prenotazione**.
- È possibile assegnare a un visitatore una selezione individuale di porte o gruppi porte su un supporto utente.
- In presenza di supporti utente aggiuntivi, non occorre effettuare ulteriori configurazioni dei componenti.
- Creando ulteriori gruppi, si semplificano la struttura degli impianti di chiusura e l'assegnazione dell'autorizzazione.

3.4.1 Diritti di accesso

Ai supporti utente viene assegnata un'autorizzazione singola, per un periodo limitato, per una selezione di componenti o gruppi porte. A questo scopo nei supporti utente viene memorizzata una lista di gruppi porte o porte.

Diritto gruppi porte
I diritti di gruppi porte possono essere raggruppati su base organizzativa (secondo le persone) o di spazi (secondo le parti dell'edificio).

Un diritto gruppi porte è un'autorizzazione di accesso con un profilo orario superiore. Per un diritto gruppi porte, più persone o più porte vengono raggruppate in un gruppo porte. Il gruppo porte viene memorizzato nei componenti come mezzo di identificazione e al gruppo porte viene assegnato un profilo orario. Successivamente questo gruppo porte può essere assegnato ai supporti utente, consentendo così l'accesso a tutte le porte assegnate a questo gruppo porte.
Per l'autorizzazione CardLink sono disponibili 15 profili orari rispettivamente con 12 finestre orarie e il profilo orario "Sempre" costantemente valido. A ogni gruppo porte può essere assegnato un profilo orario corrispondente.

Applicazioni:

- Per grandi impianti di chiusura con molti utenti e porte. La configurazione dei gruppi porte consente di organizzare e gestire chiaramente l'Impianto di chiusura.
- Per un gruppo di persone che deve ricevere un'autorizzazione di accesso per un gruppo porte uguale a quella per i team leader e il personale di servizio.

Diritto singolo
Un diritto singolo è un'autorizzazione di accesso con un profilo orario personalizzato valido per una porta singola o un gruppo porte.

Il profilo orario di un diritto singolo è salvato sui supporti utente. Con un diritto singolo è possibile selezionare individualmente il profilo orario rispetto al gruppo porte (diritto gruppi porte).

Sono disponibili 2 varianti:

1 Diritto singolo per porte singole
È possibile assegnare ai supporti utente di una porta un'autorizzazione di accesso con profili orari personalizzati.

2 Diritto singolo per gruppo porte
È possibile assegnare ai singoli utenti (ai relativi supporti utente) di un gruppo porte un'autorizzazione di accesso con profili orari personalizzati.

Applicazioni:

- Per piccoli impianti di chiusura con pochi utenti e porte.
- Per diversi utenti, che devono ricevere l'autorizzazione di accesso personalizzata sulle singole porte, come quella per il personale addetto alle pulizie e alla sicurezza.
- Per utenti singoli che devono ricevere l'autorizzazione di accesso personalizzata per un gruppo porte uguale a quella per i team leader e il personale di servizio.

Prenotazione

Una prenotazione è un'autorizzazione di accesso per visitatori come nel caso del diritto singolo, tuttavia con l'aggiunta di una data di inizio e di fine o di un periodo di validità.

Applicazioni:

- La prenotazione è un'autorizzazione temporanea ed è utilizzata per clienti, visitatori e fornitori.

Prioritizzazione dei diritti

I diritti sono prioritizzati. I diritti sono prioritizzati consentendo di limitare o ampliare l'autorizzazione di accesso di un supporto.

I diritti vengono elaborati nella seguente successione.

- Diritto singolo
- Prenotazione
- Diritto gruppi porte

Il passaggio alla valutazione del diritto successivo avviene soltanto se non si individuano diritti "temporalmente errati". In caso contrario, la verifica viene subito interrotta.

Tuttavia, all'interno della valutazione del diritto gruppi porte la ricerca viene eseguita finché: a) tutti i diritti sono stati controllati oppure, b) viene individuato un diritto valido (gruppo porte e profilo orario corrispondente).

Esempio funzionale

Di seguito sono riportati alcuni esempi dei vari diritti di accesso.

Le condizioni sono le seguenti:

- Gruppo di porte A --> profilo orario 1
- Diversi componenti --> gruppo di porte A
- Porta "Ingresso" --> Profilo orario da 1 a 15

Esempio diritti di accesso:

Diritti di accesso	Supporto con dati	Accesso per	
		Gruppo porte A	**"Ingresso" porta**
Diritto gruppi porte	Gruppo porte A	✓ durante il profilo orario 1	✗
Diritto singolo del gruppo porte A	Gruppo porte A + profilo orario 4	✓ durante il profilo orario 4	✗
Diritto singolo della porta	"Ingresso" + profilo orario 3	✗	✓ durante il profilo orario 3
Prenotazione del gruppo porte A	Gruppo porte A + profilo orario 2 dall'inizio alla fine	✓	✗

Diritti di accesso	Supporto con dati	Accesso per	
		durante il profilo orario 2 dall'inizio alla fine	
Prenotazione della porta	"Ingresso" + profilo orario 7 dall'inizio alla fine	✗	✓ durante il profilo orario 7 dall'inizio alla fine
Combinazione tra diritto gruppi porte e Diritto singolo	Gruppo porte A "Ingresso" + profilo orario 3	✓ durante il profilo orario 1	✓ durante il profilo orario 3

3.4.2 Convalida

La convalida (time stamp sui supporti utente) è l'attivazione di un'autorizzazione di accesso. L'accesso è possibile solo con un'autorizzazione CardLink valida e con ladurata della convalida [▸ 3.4.3] attivata.

Vantaggi

- I supporti utente persi possono essere bloccati in modo rapido e semplice mediante convalida.
- L'autorizzazione CardLink scade allo scadere della durata della convalida. Questo invalida l'autorizzazione di accesso e la convalida. La convalida non può più essere rinnovata.

3.4.3 Convalida dei supporti

Convalida con i componenti standalone
I componenti standalone possono essere utilizzati anche come componenti di convalida. I componenti di convalida possono essere configurati per la convalida dell'autorizzazione CardLink. Modificando la convalida, occorre aggiornare i componenti con il Programmer 1460 o tramite wireless.

Poiché la convalida richiede energia in più, si consiglia di utilizzare solo componenti provviste di alimentazione elettrica esterna. Sono adatti, ad es. i lettori remoti, i lettori compatti o c-lever con S-Modulo.

Convalida con reader di aggiornamento wireless
I supporti utente possono essere convalidati su uno o più reader di aggiornamento wireless. Contemporaneamente la convalida o l'autorizzazione di accesso di supporti utente persi possono essere revocate nella stessa sede. I dati di convalida sono gestiti dal software di sistema e trasferiti tramite wireless al reader di aggiornamento.

Convalida con terminale
I supporti utente possono essere convalidati su uno o più terminali di convalida. Contemporaneamente è possibile ritirare la convalida o l'autorizzazione di accesso di supporti utente persi direttamente su un terminale. Il terminale viene gestito dal software di sistema.

Durata della convalida
Con la convalida effettuata presso un terminale o un componente di convalida, sui supporti utente viene apposto un time stamp. A partire da questo momento, l'autorizzazione di accesso per componenti standalone CardLink è valida.

Alla presentazione dei supporti utente viene verificato il periodo di validità dei supporti. Questo significa che l'accesso viene assegnato solo se il periodo di validità non è scaduto e l'autorizzazione temporale per il gruppo porte o la porta corrispondente (conformemente al profilo orario) è disponibile.

Sono applicabili i seguenti tipi di convalida:

Tipi di convalida	Stato
Durata in giorni e ore	In giorni e ore. (valore max 999 gg. e 24 h)
24 ore (1 giorno)	Questo tipo non è modificabile.
Orario di fine giornata (h)	Fino a un determinato orario.
"Sempre"	Questo tipo non è modificabile.

Per il tipo di convalida "Sempre" non è più possibile disattivare i supporti utente persi. Quindi i supporti utente persi devono essere registrati obbligatoriamente a tempo indeterminato nella blacklist [▶ 3.4.5] dei componenti.
Lo spazio di memoria per la registrazione dei supporti persi nella blacklist è limitato.
Questa tipologia di convalida non è consigliata per l'applicazione.

Modalità di convalida
Le modalità di convalida si differenziano tra tipo di supporti e tipo di componenti. La modalità di convalida viene impostata sempre sul componente. In un impianto di chiusura è possibile utilizzare entrambe le modalità di convalida.

Tipo supporti (standard)
La durata della convalida viene creata in modo predefinito su tutti i supporti utente. Al momento della presentazione dei supporti utente sui componenti, il time stamp attuale e la durata della convalida dei supporti utente vengono letti e confrontati con l'ora attuale del componente. Se l'orario attuale è precedente al time stamp e alla durata, la convalida è valida. Se posteriore, il tempo di convalida è ritenuto scaduto e il supporto non valido.

Tipo di componenti
La durata della convalida viene memorizzata sui componenti. Al momento della presentazione dei supporti utente sui componenti, solo il time stamp attuale dei supporti utente viene letto e confrontato con l'ora attuale dei componenti. Se l'ora rientra nella durata della convalida, l'autorizzazione dei supporti utente è valida. Se posteriore, il tempo di convalida è ritenuto scaduto e il supporto non valido e non più autorizzato.

Sono possibili le seguenti modalità di convalida:

Modalità di convalida	Durata della convalida stabilita da	da aggiornare Time stamp
Supporti (standard)	Supporti	sui supporti
Componenti	Componenti	sui supporti

Esempio funzionale
In un impianto di chiusura viene selezionato il tempo di convalida di 48 ore memorizzato nei supporti utente. Ad ogni accesso all'ingresso principale, i supporti utente vengono aggiornati ricevendo l'accesso per le porte dell'edificio. I collaboratori automuniti utilizzano il parcheggio dell'area esterna, che è protetto da una sbarra. Poiché non è possibile eseguire la convalida sul componente della sbarra, le convalide di 48 ore non sono più valide dopo i fine settimana o le ferie. La sbarra rimarrebbe chiusa. In questo caso è possibile configurare la sbarra con la convalida dei componenti, che consente di impostare una durata della convalida di 4 settimane. In questo modo si garantisce che la sbarra si apra anche con un time stamp di 3 settimane.

3.4.4 Supporti persi

Ai supporti utente persi non viene più aggiornata la convalida. Pertanto questi supporti non sono più validi e l'accesso viene bloccato.

Esistono 4 possibilità per escludere i supporti persi:

- Nel caso dei terminali, il supporto viene impostato sullo stato "Perso" nel software di sistema e non viene più convalidato dal terminale successivamente.
- Nel caso dei componenti di convalida, il supporto viene registrato nella blacklist. Il supporto perso non può più essere convalidato. Tuttavia la validità del supporto cessa soltanto allo scadere della durata della convalida.
- Se il supporto è in funzione con componenti standalone, viene registrato nella blacklist. Successivamente i dati vengono trasmessi a tutti i componenti standalone degli impianti interessati con il Programmer, un supporto di servizio o, se disponibile, tramite wireless.

- Se si utilizzano componenti wireless, dopo la cancellazione del supporto perso nel software di sistema viene trasmessa una nuova parametrizzazione ai componenti.

3.4.5 Blacklist

La funzione Blacklist consente di bloccare i supporti utente su tutti i componenti (di convalida) standalone.

Nel caso in cui occorra bloccare i supporti utente entro il periodo di validità di una convalida, è necessario procedere con il Programmer 1460 o un supporto di servizio su tutti i componenti standalone dell'impianto corrispondente. Successivamente è possibile eseguire la riconferma nel software di sistema con il Programmer 1460 o il supporto di servizio corrispondente.

È possibile eseguire il blocco anche tramite la catena di strumenti software di sistema – Programmer o tramite wireless.

3.4.6 Supporti di servizio

I supporti di servizio sono possibili solo per KEM.

Per poter utilizzare dei supporti come supporti di servizio, devono essere definiti come tali mediante il software di sistema. A tal fine sono disponibili schede funzione, identificabili grazie al loro layout caratteristico.



I supporti utente persi possono essere inseriti in Blacklist [▶ 3.4.5] con il software di sistema. L'inserimento nella blacklist viene trascritto sul supporto di servizio e trasferito con esso ai componenti. La riconferma avviene leggendo nuovamente il supporto di servizio nel software di sistema.

3.4.7 Informazione sullo stato

Le informazioni di stato sono informazioni supplementari trasmesse dal componente ai supporti. Se il livello di batteria di un componente è troppo basso, tale informazione di stato viene scritta sui supporti. Se i supporti con informazioni di stato vengono letti da un lettore da tavolo o da un terminale, tali informazioni vengono inoltrate e visualizzate sul software di sistema.

Nei componenti wireless le informazioni di stato vengono inoltrate senza fili e visualizzate sul software di sistema. La procedura deve essere eventualmente avviata nel software di sistema.

3.4.8 Traceback supporti

La funzione può essere configurata nel software di sistema.

La modalità di autorizzazione CardLink consente di salvare eventi di accesso specifici del supporto sui supporti utente. È possibile leggere questi dati tramite un lettore da tavolo o un terminale e trasmetterli al software di sistema.

Per esempio vengono salvati i seguenti eventi e stati:

- Accesso con autorizzazione
- Accesso non autorizzato
- Convalida non valida
- Ora sbagliata

3.5 Access on Card

Nella modalità Access on Card (AoC), le autorizzazioni vengono salvate sul supporto utente. I dati di accesso hanno un periodo di validità che può variare a seconda delle esigenze dell'utente. Il periodo di validità può anche essere impostato come illimitato, ovvero senza data di scadenza. La modalità AoC viene impostata nell'ambiente MATRIX.

Nel caso di Data on Card, durante una registrazione i dati del componente vengono salvati sul supporto utente. Questi dati vengono letti da un lettore collegato a un sistema host per la successiva elaborazione nel sistema host.

3.6 Modalità mista

Nella modalità mista, su un supporto vengono salvate le autorizzazioni CardLink o Whitelist. Se è previsto il supporto di un componente configurato in modalità mista, il componente verifica innanzitutto l'autorizzazione Whitelist. Se non viene rilevata alcuna autorizzazione, allora procede con la verifica dell'autorizzazione CardLink. Il componente si apre se il supporto è autorizzato da una di queste autorizzazioni.

Se il supporto viene rilevato in entrambi i tipi di autorizzazione e in uno dei due risulta "non autorizzato" allora viene rifiutato.

Esempio: Il componente non si apre se un supporto presenta un'autorizzazione CardLink valida ma anche un'autorizzazione Whitelist con un profilo orario al di fuori del periodo di validità.

3.7 Supporti non autorizzati

I componenti restano chiusi se sono presentati supporti utente non autorizzati. Se nello stato aperto vengono presentati supporti utente non autorizzati, i componenti rimangono aperti. I componenti segnalano il rifiuto dei supporti non autorizzati.

3.8 Funzioni TimePro

Questo capitolo descrive le funzioni di TimePro Office e Day/Night.

Informazioni dettagliate e supplementari sulle due funzioni TimePro e sulle loro proprietà per i componenti elettronici sono descritte nelle istruzioni per l'uso del software di sistema KEM.

Per c-lever e c-lever pro le funzioni TimePro e le seguenti funzioni non possono più essere combinate:

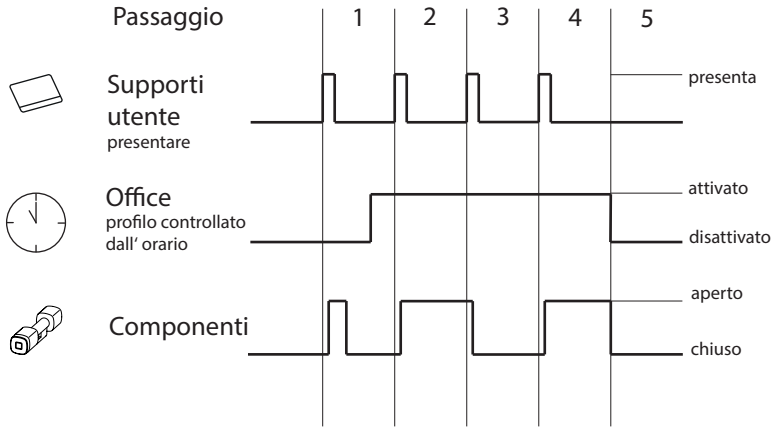
- Modalità Pass
- escape return

3.8.1 Profilo orario Office

All'interno del profilo orario TimePro inserito, i componenti possono essere impostati sullo stato di apertura da parte dei supporti autorizzati.

Nota: La funzione del profilo orario Office può essere limitata ai singoli supporti utente nel software di sistema.

Esempio funzionale



Processo 1
I componenti chiusi vengono aperti con supporti utente autorizzati. Dopo un certo tempo di apertura (alcuni secondi), i componenti si richiudono automaticamente.

Processo 2
Una volta presentati i supporti utente autorizzati, i componenti rimangono permanentemente aperti.

Processo 3
Se nello stato aperto vengono presentati supporti utente autorizzati, i componenti si chiudono nuovamente.

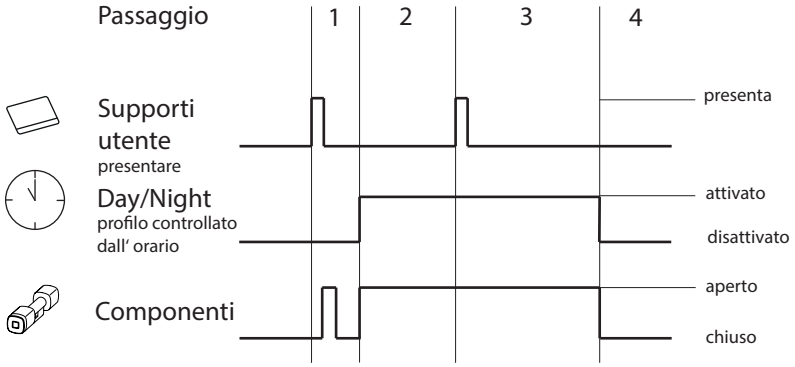
Processo 4
Dopo la ripresentazione dei supporti utente autorizzati, i componenti rimangono permanentemente aperti.

Processo 5
Una volta scaduto il profilo orario Office, i componenti si chiudono automaticamente.

3.8.2 Profilo orario Day/Night

Il profilo orario Day/Night consente di definire l'intervallo di tempo in cui i componenti si trovano in stato aperto.

Esempio funzionale



Processo 1
I componenti chiusi vengono aperti con supporti utente autorizzati. Dopo un certo tempo di apertura (alcuni secondi), i componenti si richiudono automaticamente.

Processo 2
I componenti si aprono automaticamente all'avvio del profilo orario.

Processo 3
Quando i componenti sono aperti, i supporti autorizzati o non autorizzati non hanno alcuna influenza sullo stato dei componenti. I componenti rimangono aperti e segnalano come nei supporti con autorizzazione di accesso.

Processo 4
Una volta scaduto il profilo orario, i componenti si richiudono automaticamente.

Esempio funzionale

L'autorizzazione di accesso viene concessa solo se vengono presentati supporti utente il cui UID o CID è memorizzato nei componenti.

Esempio funzionale Whitelist con profilo orario:

Componenti	**Supporti**	**Acces-so**
Lista degli UID memorizzati nei componenti e dei profili orari corrispondenti	**UID dei supporti presentati per una de-terminata data e ora**	
	Es.: Venerdì, 5 agosto 2014/10:15	
578AE976 “Sempre”	578AE976	✓
222BE121 Lunedì – Venerdì 8:00 – 17:00	222BE121	✓
829FE649 Domenica 10:00 – 12:00	829FE649	✗
—	121CA001	✗

3.9 Funzioni avanzate

3.9.1 Componenti wireless

Con la funzione wireless, i componenti standalone wireless V4 sono collegati via radio al rispettivo software di sistema.

La funzione wireless è un'opzione per i componenti standalone V4 (MRD), come il cilindro digitale e il supporto elettronico c-lever. L'opzione viene configurata con il software di sistema, ad esempio KEM.

Vantaggi

- Spese di amministrazione e gestione ridotte
- Modifica dell'autorizzazione di accesso in tempo reale
- Interrogazione e salvataggio diretti di eventi e stati
- Visualizzazione dello stato batteria
- Trasmissione wireless dell'aggiornamento firmware

Limitazioni:

- La funzione non è combinabile con TouchGo.

3.9.1.1 Panoramica

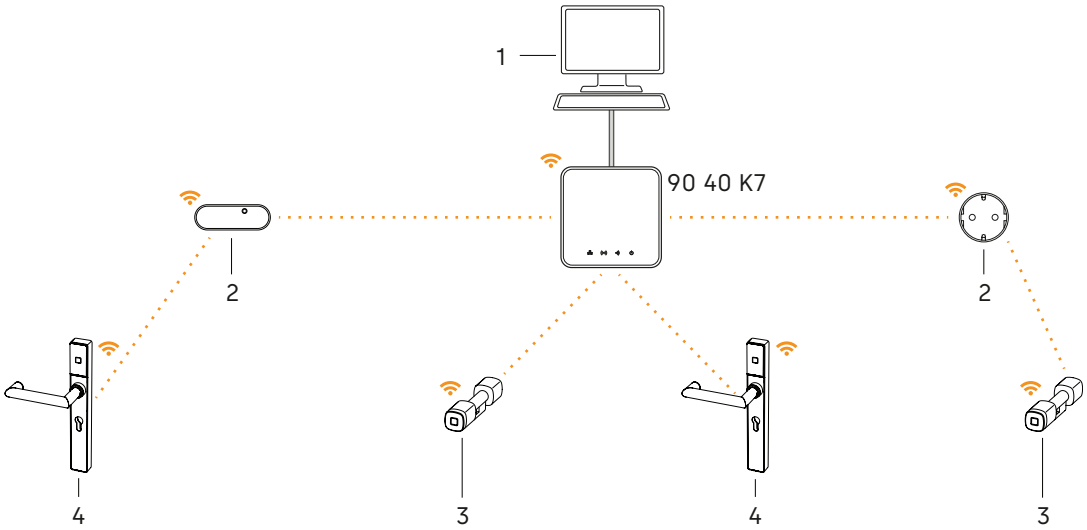
I componenti wireless sono collegati a un sistema di controllo accessi tramite il wireless gateway.

Il sistema di controllo accessi è gestito da un software di sistema. Con il software di sistema si configurano i dispositivi collegati e si assegnano i diritti di accesso.

La trasmissione dei dati al software di sistema avviene tramite la linea Ethernet. La trasmissione dei dati ai componenti wireless avviene via radio.

La portata del collegamento radio può essere estesa con Wireless Extender.

Topologia
Lo schema mostra il collegamento del gateway wireless con componenti wireless e wireless extender in un sistema dormakaba.



Dispositivo wireless
Comunicazione wireless

1 Sistema superiore
2 wireless extender
3 Componente wireless (cilindro digitale)
4 Componente wireless (c-lever pro)

1 Software di sistema
2 Wireless gateway

3 Componente della porta wireless

– A un wireless gateway è possibile collegare max. 16 componenti della porta wireless.

4 wireless extender

– A un wireless gateway è possibile collegare max. 8 Wireless Extender.

– È possibile collegare in serie max. 4 Wireless Extender.
(Wireless Gateway → 1. Wireless Extender→ ... → 4. Wireless Extender)

3.9.1.2 Misurazione con il Site Survey Tool

Lo strumento Site Survey Tool può essere utilizzato per misurare la qualità del segnale di un wireless gateway in vari punti. I risultati delle misurazioni possono essere utilizzati per determinare la posizione del gateway in modo da raggiungere tutti i componenti wireless con una qualità del segnale ottimale. Se la qualità del segnale non è sufficiente per un funzionamento affidabile, è necessario aggiungere al sistema altri gateway o extender.

Ulteriori informazioni sono disponibili nelle linee guida per la pianificazione wireless e nella descrizione del programma per il Site Survey Tool.

3.9.1.3 Misurazione della portata con supporto di test wireless

Metodo di rilevazione alternativo se non è disponibile il Site Survey Tool.

Una descrizione dettagliata della misurazione del raggio d'azione con il gateway è disponibile nelle istruzioni separate PG Wireless (linea guida di pianificazione) e nel manuale sul wireless gateway.

Supporto necessario: Supporto di prova wireless



3.9.1.4 Messa in funzione

La messa in funzione dei componenti wireless con il Programmer 1460 è descritta nei manuali del Programmer, del gateway e del software di sistema.

Principio
La messa in funzione wireless viene avviata sul gateway 90 40-K7 a cui il componente deve collegarsi. Tramite il Programmer viene avviata la sequenza di collegamento sul componente. Una volta collegato correttamente al gateway, il componente può essere configurato online con il software di sistema.

3.9.2 Componenti Traceback

Il traceback componenti è un file registro in cui vengono registrati e salvati tutti gli eventi dei componenti. È possibile disattivare la funzione nel software di sistema.

Nella memoria vengono registrati fino a 2.000 eventi. La voce più recente viene sovrascritta su quella meno recente. Ogni voce riceve un time stamp, per cui l'ora del componente deve essere impostata correttamente. Le registrazioni consentono di tracciare ogni accesso autorizzato o non consentito a una porta.

Per esempio vengono salvati i seguenti eventi e stati:

- Accesso con autorizzazione
- Accesso non consentito a causa di autorizzazione o convalida mancante
- Accesso non consentito a causa della finestra oraria errata
- Impostazione dell'ora
- Programmazione
- Test di sistema etc.

3.9.3 Modulo S

Con S-Modulo, il comportamento del componente (autorizzazione) viene sovrascritto da un contatto esterno a potenziale zero. S-Modulo viene attivato da un interruttore, da un timer o dal sistema di gestione dell'edificio (ad es. impianto di allarme). Un componente con S-Modulo può essere alimentato da un alimentatore esterno. In questo caso le batterie non sono più necessarie.

Il modulo S è possibile per i seguenti componenti:

c-lever pro	configurabile/integrabile a posteriori
Cilindro MC	integrabile a posteriori
Lettore remoto	presente come standard
Lettore compatto	presente come standard

Il modulo S viene configurato con il software di sistema.

Limitazioni:

- Le funzioni di commutazione dell'S-Modulo, il Pass-Lock e la modalità Pass non possono essere utilizzati assieme.
- L'alimentazione di tensione esterna del dispositivo è possibile con l'S-Modulo.
- La funzione non è supportata per OSS-SO.

3.9.4 Funzione di rientro (Escape Return) in c-lever pro

La funzione "Escape-Return" permette di rientrare liberamente, senza dover utilizzare i supporti, nei locali abbandonati in caso di emergenza (per es. incendio).
Infatti, il locale resta aperto nel caso qualcuno sia uscito senza portare con sé il supporto. Al momento dell'uscita, il locale può essere chiuso solo con il supporto o premendo il tasto.

Limitazioni:

- La funzione può essere utilizzata solo con componenti c-lever pro.
- La funzione non può essere utilizzata in combinazione con TimePro e Pass-Lock.
- Le funzioni di commutazione dell'S-Modulo e la funzione di rientro non possono essere utilizzati assieme.
- L'alimentazione di tensione esterna del dispositivo è possibile con l'S-Modulo.

3.9.5 Modalità Pass per c-lever pro

La modalità Pass è un'opzione disponibile per il ferramento elettronico c-lever pro. La funzione viene attivata e disattivata tramite un tasto. Premendo il tasto (non sono necessari supporti utente) la porta rimane aperta. Premendo nuovamente il tasto o presentando un supporto utente autorizzato, il ferramento elettronico della porta passa nuovamente allo stato chiuso. È possibile interrogare lo stato attuale della porta in qualsiasi momento

premendo brevemente il tasto.
Se l'hardware viene riconosciuto, vengono caricate le impostazioni preconfigurate.
La modalità Pass viene configurata con il software di sistema.

Limitazioni:

- Le funzioni di commutazione dell'S-Modulo, il Pass-Lock e la modalità Pass non possono essere utilizzati assieme.
- L'alimentazione di tensione esterna del dispositivo è possibile con l'S-Modulo.
- La funzione non è supportata per OSS-SO.
- Il funzionamento della modalità Pass wireless è supportato a partire dalla versione del firmware 42.38.

3.9.6 Pass-Lock in c-lever pro

Pass-Lock è un'opzione disponibile per il ferramento elettronico c-lever pro. La funzione viene attivata con il tasto sul ferramento. Premendo il tasto, la porta resta chiusa per le persone all'esterno. Presentando un supporto autorizzato (master o utente), c-lever pro ritorna allo stato aperto. È sempre possibile aprire la porta dall'interno.
Pass-Lock viene configurato con il software di sistema. Per evitare un'attivazione involontaria, è possibile configurare un ritardo compreso tra 0,1 e 5 secondi. Pass-Lock si attiva solo se il tasto viene tenuto premuto per l'intera durata del ritardo configurato.

Limitazioni

- Le funzioni di commutazione del modulo S, il Pass-Lock e la modalità Pass non possono essere utilizzati assieme.
- L'alimentazione di tensione esterna del dispositivo è possibile con il modulo S.
- La funzione non è supportata in caso di funzionamento con OSS-SO.
- Il funzionamento di Pass-Lock tramite wireless è supportato a partire dalla versione firmware 42.38.
- Il ritardo di attivazione è configurabile nel software di sistema. Se non viene configurato esplicitamente alcun ritardo, si applica il comportamento predefinito (nessun ritardo). Questa opzione è disponibile a partire dalla versione 42.48.

3.9.7 Supporti di intervento



Questa funzione è disponibile a partire dalla versione firmware 42.48.

I componenti evolo supportano un modello di autorizzazione a due livelli (2LA). Oltre al gruppo standard di utenti autorizzati, a un secondo gruppo di supporti, definito separatamente, possono essere assegnate autorizzazioni estese per specifiche situazioni di accesso. Questo gruppo di intervento funziona indipendentemente dall'autorizzazione standard e può ottenere l'accesso in situazioni in cui i normali supporti utente sono limitati o bloccati, ad esempio quando il Pass-Lock è attivo o quando un sistema di rilevamento delle intrusioni (IDS) è attivato. Sono supportati i seguenti casi d'uso:

Supporti di intervento per Pass-Lock
Quando il Pass-Lock è attivo, una porta viene normalmente riportata allo stato aperto solo presentando un supporto master o un qualsiasi supporto utente autorizzato. A tale scopo è possibile configurare un gruppo dedicato di supporti di intervento. A differenza di tutti gli altri utenti autorizzati, solo i membri di questo gruppo possono quindi disattivare il Pass-Lock. Questa soluzione è utile quando si desidera limitare le persone autorizzate a revocare un blocco, ad esempio al personale addetto alla sicurezza o al personale tecnico designato.

Supporti di intervento per IDS
Quando un sistema di rilevamento delle intrusioni (IDS) è attivato, normalmente tutti i supporti vengono rifiutati finché l'IDS non viene disattivato. È possibile definire un gruppo speciale di supporti di intervento che mantiene l'accesso anche quando l'IDS è attivato. In questo modo il personale designato, ad esempio i servizi di emergenza, può accedere ai locali indipendentemente dallo stato dell'allarme.

Limitazioni

- I supporti di intervento per IDS sono supportati solo in modalità wireless e richiedono un Wireless Gateway 90 40-K7 con versione firmware 5.1 o superiore.

- L'attivazione dell'IDS è una funzione MATRIX. Per i dettagli sulla configurazione, si veda la documentazione del sistema host MATRIX.
- I supporti di intervento vengono configurati con il software di sistema. Per i dettagli sulla configurazione, si veda il manuale del software di sistema.

3.9.8 Disattivazione della programmazione manuale

La programmazione manuale dei componenti con supporti è disattivata quando si utilizzano il software di sistema e il Programmer 1460.

3.10 TouchGo

Il sistema di chiusura elettronico TouchGo è un sistema di autorizzazione di accesso che può essere utilizzato come impianto indipendente o come estensione del sottosistema dormakaba evolo per un maggiore comfort. Alla base di questo comfort c'è la tecnologia RCID. Si veda il capitolo Aspetti di sicurezza [▶ 3.10.2].

Il sistema TouchGo è disponibile in due diverse varianti, che definiscono le funzioni dei componenti. Con un sottosistema evolo sono combinabili esclusivamente componenti della variante TouchGo E310.

Un sistema TouchGo consente di chiudere le porte senza dover prendere in mano chiavi o supporti utente. Toccando semplicemente il componente, il sistema riconosce se la persona ha con sé un supporto utente autorizzato. A tale scopo, è sufficiente che il supporto utente si trovi a una distanza di circa 5–10 cm dal corpo, per esempio nella tasca dei pantaloni o della giacca o nella borsa.

Limitazioni:

- TouchGo non può essere utilizzato con la funzione wireless.

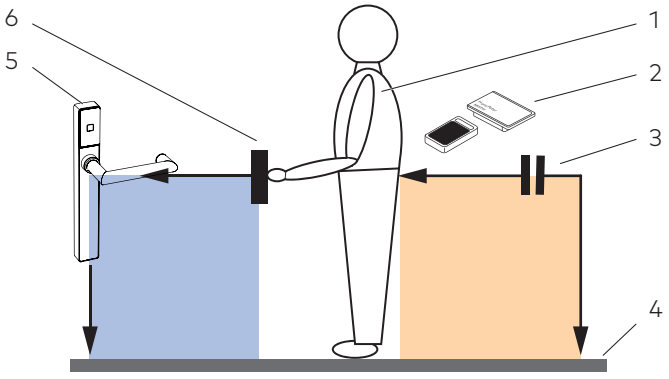
Documenti di approfondimento

- Linea guida di pianificazione dormakaba c-lever pro TouchGo con modulo S
- Istruzioni per l'uso di dormakaba c-lever pro TouchGo

3.10.1 Funzionamento RCID

RCID: Resistive Capacitive Identification

Al contatto con il componente (6–5) viene identificato un supporto RCID (2) indossato e ne viene valutata l'autorizzazione.



1 Persona
2 Supporti RCID
3 Trasmissione capacitiva del segnale (arancione)
4 Dimensioni comuni (pavimento)
5 Componente TouchGo
6 Trasmissione resistiva del segnale tramite maniglia (blu)

3.10.2 Aspetti di sicurezza

La tecnologia RCID si distingue dalle soluzioni convenzionali in quanto il trasferimento delle informazioni avviene tramite il campo elettrostatico del corpo [▶ 3.10.1] senza limitare né il comfort né la sicurezza. Allo stesso tempo, sono mantenute le funzioni flessibili e sicure dei sistemi di chiusura elettronici. Si vedano il capitolo Sicurezza con le abilitazioni CardLink LEGIC [▶ 5.2] e il capitolo Sicurezza con l'autorizzazione della whitelist LEGIC [▶ 5.3].

La sicurezza dell'intero sistema è garantita in ogni momento con TouchGo, in quanto un supporto utente perso si può cancellare in modo semplice e veloce. Ciò consente allo stesso tempo di evitare non solo le falle di sicurezza ma anche una costosa sostituzione dell'intero impianto di chiusura.

3.10.3 TouchGo E110

TouchGo E110 può essere utilizzato con i supporti corrispondenti per un massimo di 100 utenti. È dotato di funzione modalità Office TouchGo. TouchGo E110 è completamente funzionante senza dispositivi di programmazione e software di sistema.

TouchGo E110 è standalone e non può essere utilizzato in un sottosistema evolo.

La programmazione di TouchGo E110 è descritta nelle istruzioni per l'uso di c-lever pro TouchGo.

3.10.4 TouchGo E310

I componenti TouchGo E310 possono essere collegati facilmente al software di sistema scelto, senza perdite in termini di sicurezza. TouchGo E310 è un'opzione comfort che non influisce minimamente su un dispositivo di sicurezza.

Per garantire un'identificazione e una gestione univoca, il sottosistema evolo ricorre alla comprovata tecnologia RFID. A questo scopo, durante la lettura, i dati RFID del componente vengono "accoppiati" con i dati della tecnologia TouchGo (pairing). Ciò significa che l'autorizzazione di accesso assegnata viene trasmessa a TouchGo e il componente la riconosce al contatto.

Le modifiche future dell'autorizzazione, trasmesse tramite il programmer (autorizzazione Whitelist) o la tecnologia RFID (autorizzazione CardLink), vengono acquisite automaticamente in TouchGo. In caso di perdita o guasto del supporto combinato o di esclusione del partner di pairing, l'autorizzazione può essere immediatamente cancellata. In casi diversi, si può continuare a utilizzare i singoli componenti, poiché in qualunque momento è possibile eseguire un nuovo "accoppiamento" direttamente sui componenti.

TouchGo non può essere utilizzato con la funzione wireless.

3.10.4.1 Autorizzazione whitelist con TouchGo

Negli impianti di chiusura con autorizzazione Whitelist è possibile utilizzare l'opzione comfort aggiuntiva di TouchGo per i componenti TouchGo. Il supporto combinato RFID/RCID TouchGo,come il supporto RFID, può essere programmato nel componente semplicemente tramite i supporti di programmazione RFID oppure può essere appoggiato sul lettore da tavolo per registrare i dati della tecnologia RFID nel software di sistema. L'autorizzazione di accesso della tecnologia RFID viene assegnata ai componenti mediante il programmer. Il supporto combinato viene presentato al componente standalone e "accoppiato" (pairing) alla tecnologia TouchGo durante la lettura dei dati RFID. La stessa autorizzazione di accesso viene trasmessa a TouchGo e il componente riconosce l'autorizzazione al contatto.

Le modifiche future dell'autorizzazione vengono acquisite automaticamente in TouchGo.

3.10.4.2 Autorizzazione CardLink con TouchGo

Anche negli impianti di chiusura con autorizzazioni CardLink è possibile utilizzare l'opzione comfort aggiuntiva di TouchGo per i componenti TouchGo. La concessione delle autorizzazioni avviene nel software di sistema e viene trasmessa ai componenti standalone tramite tecnologia RFID.

Contemporaneamente TouchGo viene "accoppiato" (pairing) per la trasmissione. Ciò significa che l'autorizzazione di accesso assegnata viene trasmessa a TouchGo e il componente la riconosce al contatto.

Le modifiche future dell'autorizzazione e il rinnovo della convalida vengono trasmessi ai componenti standalone tramite la tecnologia RFID e, contemporaneamente, viene verificato l'"accoppiamento" (pairing).

3.11 Selezione libera dell'armadietto con serratura per armadietti 21 10 e 21 20

Questa opzione è disponibile solo con i modelli di serratura per armadietti 21 10 e 21 20.

Nella modalità di accesso CardLink o Whitelist, l'autorizzazione per un armadietto viene assegnata all'utente come per un normale componente. Nella modalità di accesso 'Selezione libera dell'armadietto con CardLink' o 'Selezione libera dell'armadietto con Whitelist' sono gli utenti stessi a occupare un armadietto libero per il quale sono autorizzati. Deve essere configurata una modalità di accesso. Il numero di armadietti occupabili dal singolo utente viene stabilito sul supporto utente tramite la procedura guidata per le serrature per armadietti. È possibile occupare da uno a quattro armadietti. Un armadietto occupato si può aprire solo con il supporto utente corrispondente o con un supporto di servizio. La scelta dell'utente viene quindi cancellata e l'armadietto risulta nuovamente libero.

Le assegnazioni degli armadietti possono essere cancellate con gli strumenti di gestione del sistema host, ad esempio con la procedura guidata per le serrature per armadietti in dormakaba evolo Manager (KEM).

3.12 Cassetta lettere/ascensore

Con il supporto utente, un utente può aprire solo le cassette delle lettere oppure in ascensore può raggiungere solamente i piani per i quali è autorizzato.

È possibile configurare Cassetta lettere/ascensore solo tramite il software di sistema.
Mobile Access è possibile dalla versione FW 42.38
Ciò non è possibile tramite wireless.

Un'unità consiste di un lettore remoto 91 15 e di un massimo di 6 moduli 90 30 con 8 uscite attivate ciascuno. Il numero di moduli dipende dal numero delle uscite necessarie. In questo modo può essere configurato un massimo di 49 uscite.

Rapporto tra le uscite ed i componenti necessari:

Numero uscite	Numero componenti
1	91 15 (lettore remoto con 1 uscita a relè)
fino a 9	91 15 + 1 x 90 30 (modulo d'ampliamento con 8 uscite a relè)
fino a 17	91 15 + 2 x 90 30
fino a 25	91 15 + 3 x 90 30
fino a 33	91 15 + 4 x 90 30
fino a 41	91 15 + 5 x 90 30
fino a 49	91 15 + 6 x 90 30

4 Varianti di sistema

Il sottosistema evolo può essere impiegato in diverse varianti di sistema e rimane ampliabile in tutte le varianti.

Gli esempi scelti si riferiscono sia ai supporti LEGIC che MIFARE, anche se nelle foto viene rappresentato prevalentemente LEGIC. La differenza sta nelle tessere di sicurezza utilizzate. Per LEGIC si utilizzano le tessere di sicurezza C1 e C2, per MIFARE invece la tessera di sicurezza C.

4.1 Programmazione whitelist

4.1.1 Autorizzazione whitelist senza catena degli strumenti

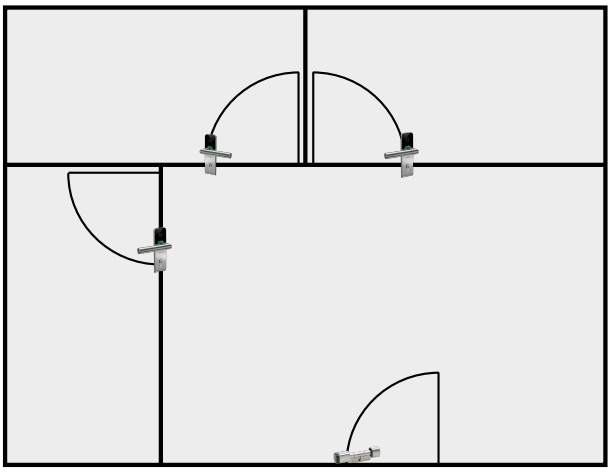
Negli impianti di chiusura di piccole dimensioni, i supporti utente vengono programmati con un master direttamente nei componenti. Per questo metodo non è necessario il software di sistema , né il programmer, Non sono possibili neanche il wireless o Mobile Access.

La programmazione viene descritta nel capitolo Programmazione con supporti.

Master A, master B e supporti utente



Esempio di impianto:

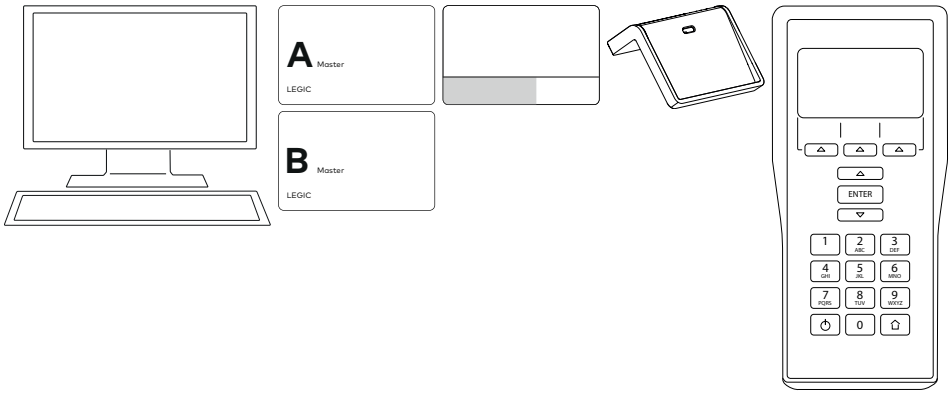


4.1.2 Autorizzazione whitelist con catena degli strumenti

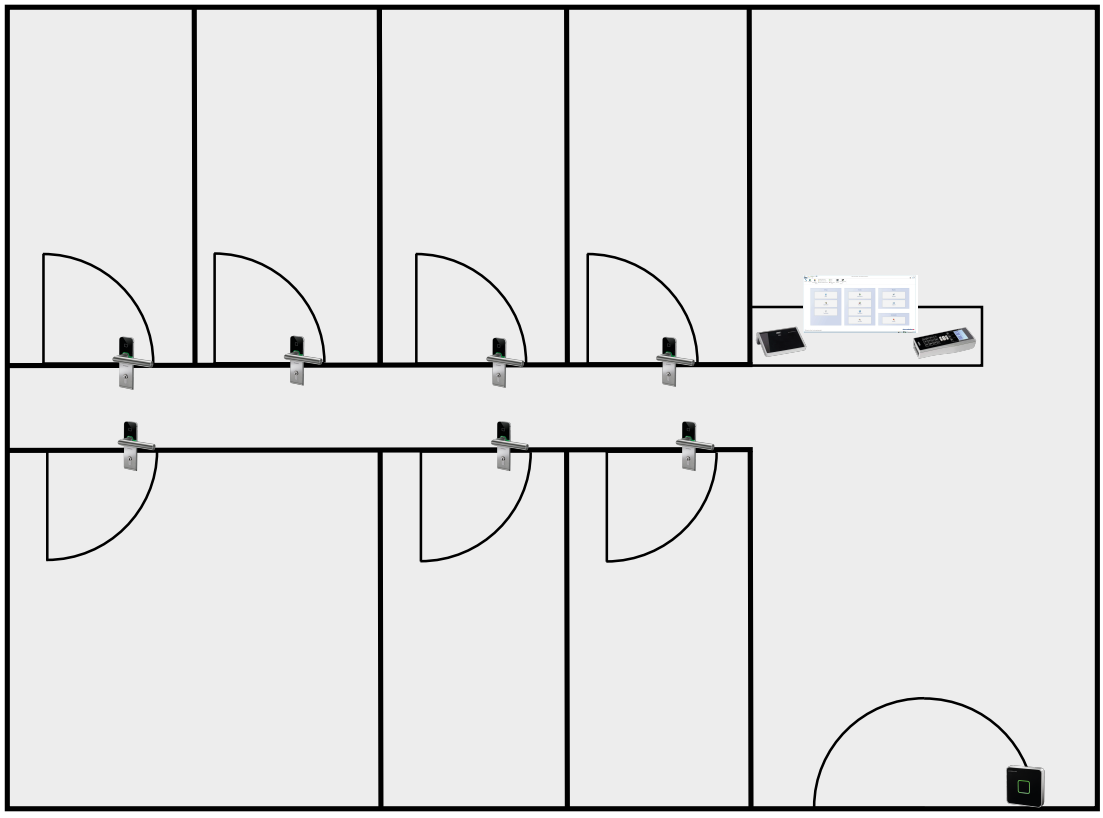
Negli impianti di chiusura di maggiori dimensioni con gestione temporale, i supporti utente vengono gestiti con il software di sistema. I dati di autorizzazione vengono trasmessi dal software ai componenti con il programmer o aggiornati tramite wireless. Nell'esempio senza wireless.

La programmazione è descritta nel capitolo Programmazione con il software di sistema e Programmer [▶ 7.5.2].

Catena di strumenti: Software di sistema con master, supporti utente, lettore da tavolo e Programmer



Esempio di impianto:



4.2 Programmazione CardLink

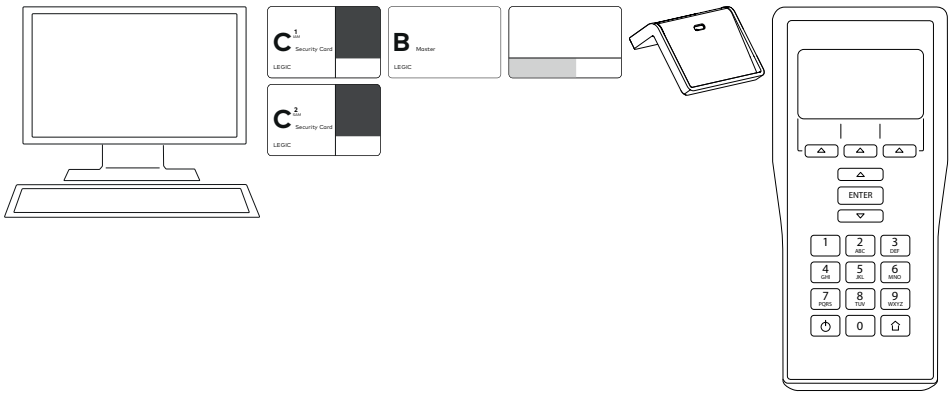
CardLink viene programmato per mezzo del software di sistema.

La programmazione è descritta nel capitolo Programmazione con il software di sistema.

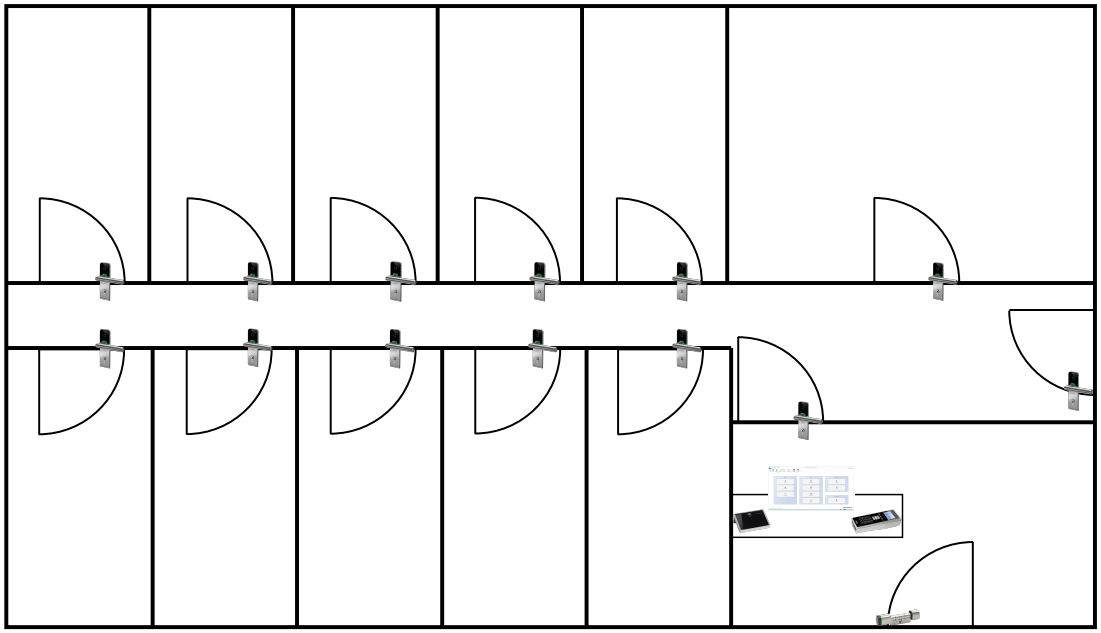
4.2.1 Autorizzazione CardLink tramite lettore da tavolo

Negli impianti di chiusura CardLink, i supporti utente vengono organizzati con il software di sistema . Le autorizzazioni vengono scritte nei supporti utente tramite il lettore da tavolo. Quanto ai componenti, è sufficiente inizializzarli per CardLink. Le nuove autorizzazioni vengono trasmesse dal software di sistema ai supporti utente tramite il lettore da tavolo. In questo caso, le convalide vengono acquisite dai singoli componenti standalone appositamente configurati. È supportata anche la funzione wireless.

Catena di strumenti: Software di sistema con tessera di sicurezza, master, supporti utente, lettore da tavolo e programmer



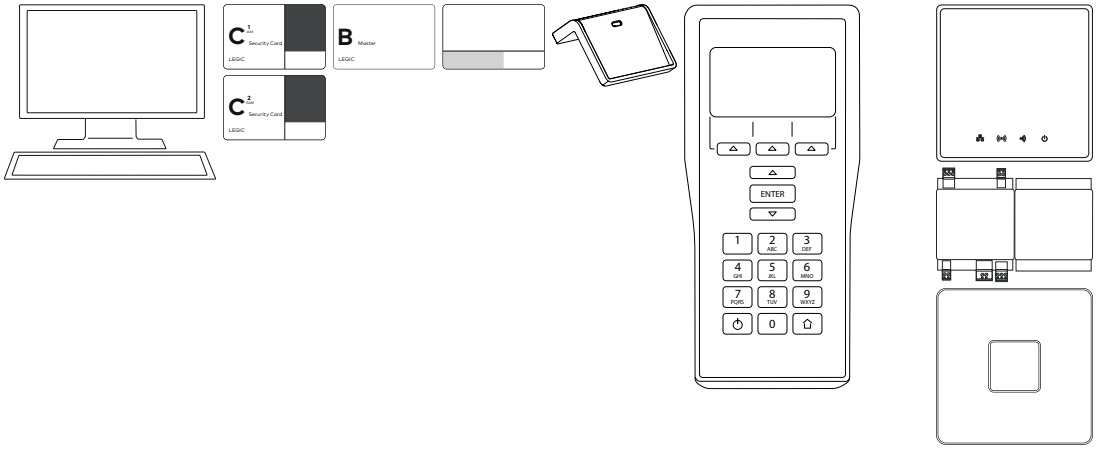
Esempio di impianto:

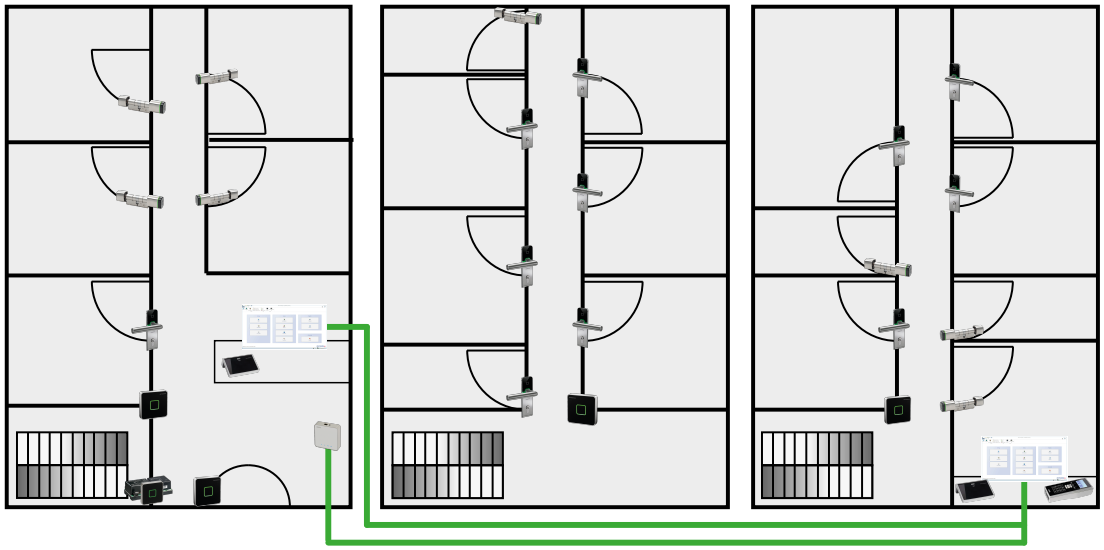


4.2.2 Autorizzazione CardLink tramite lettore di aggiornamento

Per assegnare nuove autorizzazioni di accesso nei supporti utente, al posto del terminale viene utilizzato un reader di aggiornamento Cardlink. Il reader è connesso al software di sistema tramite un wireless gateway*. In questo modo è possibile accordare o negare online nuove autorizzazioni di accesso per gli utenti indipendentemente dall'orario. In questo caso, le convalide vengono acquisite dal reader di aggiornamento.

Catena di strumenti: Software di sistema con tessera di sicurezza, master, supporti utente, lettore da tavolo, programmer, gateway e reader di aggiornamento 91 15 con modulo d'ampliamento 90 43.





Trasferire abilitazioni CardLink al lettore di aggiornamento senza wireless gateway

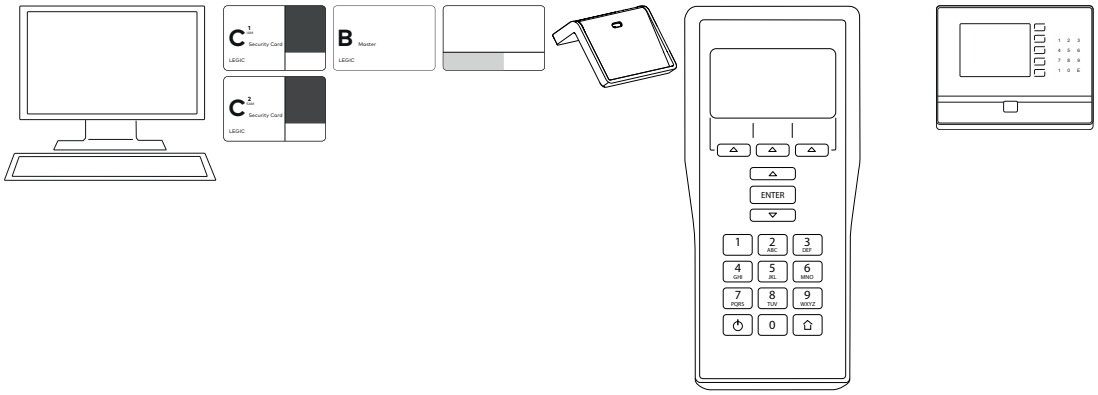
Le abilitazioni CardLink possono essere trasferite al lettore di aggiornamento con il Programmer 1460.

In questo modo si perde la comodità delle autorizzazioni di accesso online indipendenti dall'orario.

4.2.3 Autorizzazione CardLink tramite terminale

Questa modalità di autorizzazione CardLink è particolarmente idonea per impianti di chiusura con modifiche cicliche delle autorizzazioni utente. Per assegnare nuove autorizzazioni di accesso nei supporti utente viene utilizzato il terminale connesso al software di sistema. In questo modo è possibile accordare o negare nuove autorizzazioni di accesso per gli utenti indipendentemente dall'orario. In questo caso, le convalide vengono acquisite dal terminale.

Catena di strumenti: Software di sistema con tessera di sicurezza, master, supporti utente, lettore da tavolo, programmer e terminale



Esempio di impianto:



4.3 Panoramica delle varianti firmware

Funzione/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	fino a 200	fino a 200	fino a 200	fino a 200	fino a 200	fino a 200	fino a 200	fino a 200
Autorizzazioni Whitelist								
Voci Whitelist (UID/Card ID) – modalità offline	4000	1000	1000[5]	4000	4000 (modalità offline)	4000	4000 (modalità offline)	4000 (modalità offline) fino a 30.000 (utilizzo online con gateway 90 40-K7)
Voci Whitelist (UID/Card ID) – modalità online con Wireless Gateway 90 40-K7				fino a 30.000	fino a 30.000		fino a 30.000	fino a 30.000
Autorizzazioni a tempo	✓	✓	✓	✓	✓	✓	✓	✓
Disattivare la programmazione manuale	✓	✓	✓	✓	✓	✓	✓	✓
Autorizzazioni CardLink								
Convalida	✓	—	✓	✓	✓	✓	✓	✓
Diritto singolo per porta[4]	fino a 60	—	fino a 60	fino a 60	fino a 60	fino a 60	fino a 60	fino a 60
Diritto singolo per gruppo porte[4]	fino a 39	—	fino a 39	fino a 39	fino a 39	fino a 39	fino a 39	fino a 39
Prenotazione diritto singolo per porta[4]	fino a 18	—	fino a 18	fino a 18	fino a 18	fino a 18	fino a 18	fino a 18
Prenotazione diritto singolo per gruppo porte[4]	fino a 11	—	fino a 11	fino a 11	fino a 11	fino a 11	fino a 11	fino a 11
Diritto gruppi porte	512	—	512	512	512	512	512	512
Voci Blacklist	400	—	400	400	400	400	400	400
Supporti di servizio	✓	—	✓	✓	✓	✓	✓	✓
Traceback supporti[3]	60	—	60	60	60	60	60	60
Supporti TouchGo	—	—	1000	—	—	—	—	—
Funzioni avanzate								
Wireless	—	—	—	✓	✓	—	✓	✓
Memoria traceback componenti	2000	2000	2000	2000	2000	2000	2000	2000

Funzione/Firmware	E300[A]	E305[B]	E310[C]	E320[D]	E321[E]	E340[F]	E360[G]	E361[H]
Modalità Pass[1]	Opzione	—	Opzione	Opzione	Opzione	Opzione	Opzione	Opzione
Profili orari	15 e “Sempre”	15 e “Sempre”	15 e “Sempre”	15 e “Sempre”	15 e “Sempre”	15 e “Sempre”	15 e “Sempre”	15 e “Sempre”
Finestra oraria per ogni profilo orario	12	12	12	12	12	12	12	12
Periodi di ferie	20	20	20	20	20	20	20	20
Giorni particolari A+B	32+32	32+32	32+32	32+32	32+32	32+32	32+32	32+32
Funzioni TimePro	✓	✓	✓	✓	✓	✓	✓	✓
Modulo S[2]	Opzione	—	Opzione	Opzione	Opzione	Opzione	Opzione	Opzione
Master T e supporto di servizio	✓	✓	✓	✓	✓	✓	✓	✓
Mobile Access								
NFC/HCE	✓	—	—	✓	✓	✓	✓	✓
Bluetooth	—	—	—	—	—	✓	✓	✓

Legenda:

1 Solo per c-lever pro.

2 Standard per lettore, opzione per c-lever pro.

3 Solo con supporti MIFARE DESFire e LEGIC advant.
A seconda delle dimensioni del segmento/file
Valore predefinito a seconda delle specifiche del supporto. Può essere superiore o inferiore.

4 A seconda dei tipi di autorizzazione utilizzati.

5 RCID e RFID.

A E300 – evolo V4

B E305 – Cassetta lettere/ascensore
E345 – Cassetta lettere/ascensore con Mobile Access

C E310 – TouchGo

D E320 – Wireless

E E321 – Wireless con monitoraggio porta
Sono necessari componenti aggiuntivi, come contatti sul telaio della porta e sensori della serratura (scrocco, catenaccio).

F E340 – Mobile Access

G E360 – Wireless e Mobile Access

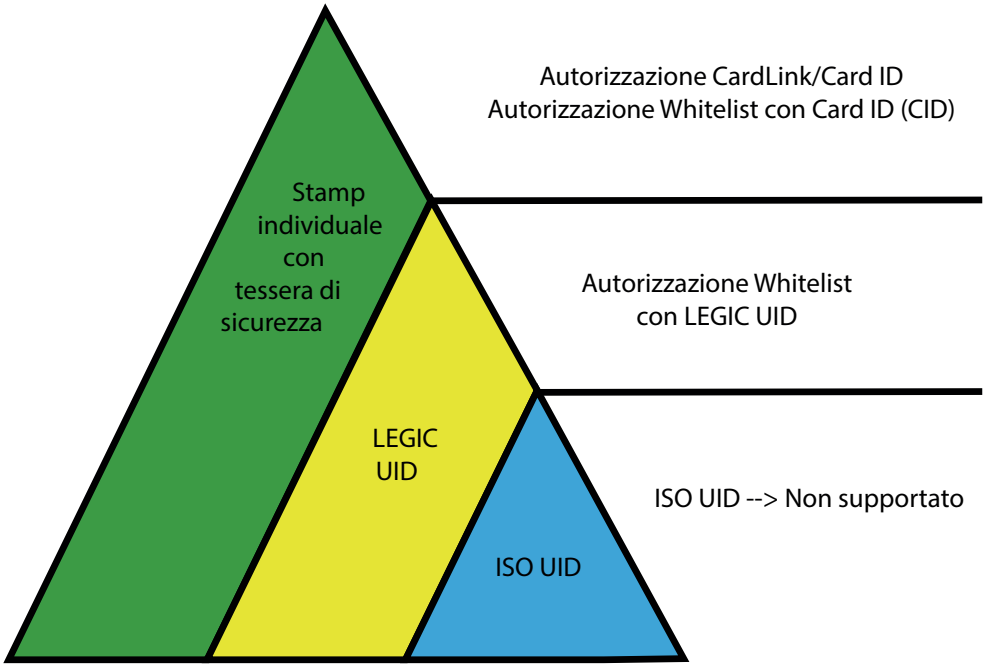
H E361 – Wireless con monitoraggio porta e Mobile Access
Sono necessari componenti aggiuntivi, come contatti sul telaio della porta e sensori della serratura (scrocco, catenaccio).

5 Funzioni di sicurezza

Questo capitolo descrive le possibili funzioni di sicurezza per LEGIC e MIFARE negli impianti di chiusura, che possono essere selezionate in base ai requisiti di sicurezza desiderati.

5.1 I livelli di sicurezza LEGIC

Per i tipi di autorizzazioni sono disponibili i seguenti livelli di sicurezza.



Stamp personalizzato
Per ogni impianto di chiusura viene definito uno stamp individuale. Questo stamp viene utilizzato per identificare il supporto LEGIC specifico dell'impianto. Lo stamp è definito dalla tessera di sicurezza C1 o C2 del rispettivo impianto di chiusura.

UID LEGIC
L'UID LEGIC viene utilizzato per i normali impianti di chiusura con una whitelist. Con LEGIC UID, il numero unico (UID) viene ulteriormente verificato tramite una funzione LEGIC sul supporto.

Nota: Il software di sistema KEM utilizza esclusivamente l'UID LEGIC.

5.2 Sicurezza con le abilitazioni CardLink LEGIC

Stamp personalizzato
Con l'utilizzo di un'autorizzazione CardLink con LEGIC, diventa necessario uno stamp personalizzato.

Ogni componente elettronico e il lettore da tavolo sono dotati di hardware LEGIC che funzionano con questo stamp. L'integrazione dello stamp specifico nell'impianto di chiusura richiede l'utilizzo della tessera di sicurezza C1 e/o C2, che trasmette lo stamp al componente corrispondente Per ogni impianto di chiusura è necessario impiegare una nuova tessera di sicurezza. Utilizzando uno stamp, occorre inizializzare il software di sistema KEM, il lettore da tavolo e i componenti corrispondenti. Successivamente la tessera di sicurezza deve essere conservata in un luogo sicuro (es. una cassaforte).

5.3 Sicurezza con l'autorizzazione della whitelist LEGIC

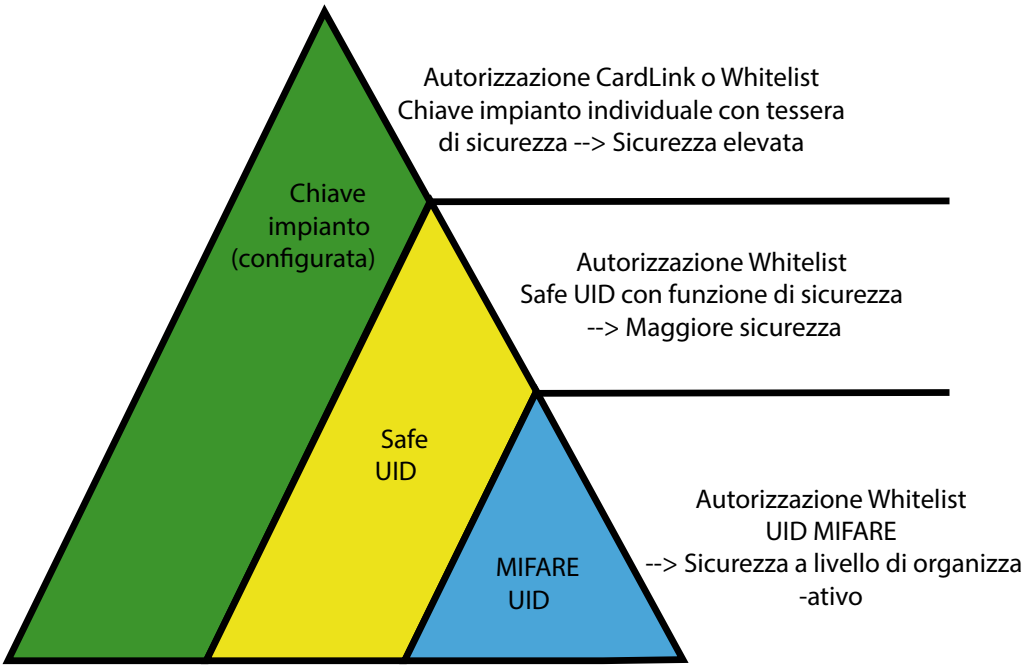
Card ID (CID)
Al posto dell'UID, il sistema assegna un CID personalizzato ai supporti.

Tale CID viene scritto nella memoria del supporto con uno stamp LEGIC personalizzato definito dalla tessera di sicurezza C1. Per ogni impianto è necessaria una nuova tessera a garanzia della sicurezza. Utilizzando lo stamp LEGIC personalizzato, occorre inizializzare il software di sistema KEM e il lettore da tavolo. Successivamente la tessera di sicurezza deve essere conservata in un luogo sicuro (es. una cassaforte).

UID LEGIC
Con l'UID LEGIC, la funzione LEGIC viene utilizzata per il salvataggio dell'UID (numero unico) dei supporti utente. La sicurezza di un UID viene sensibilmente migliorata in quanto la funzione LEGIC verifica l'UID.

5.4 I livelli di sicurezza MIFARE

Per i tipi di autorizzazioni sono disponibili i seguenti livelli di sicurezza.



Chiave dell'impianto (Sitekey)
La chiave dell'impianto è adatta all'impiego in impianti di chiusura con elevati requisiti di sicurezza.

La chiave dell'impianto è una chiave specifica che viene assegnata individualmente a ciascun impianto di chiusura. Questa chiave viene generata automaticamente da un chip di sicurezza. Questo chip di sicurezza aggiuntivo è integrato in ogni componente e, dopo l'inizializzazione, controlla la crittografia e la decrittografia individuale di tutti i dati scritti dal sistema sul supporto utente.

Safe UID
Questo livello di sicurezza è utilizzato per i normali impianti di chiusura.

Con Safe UID, anche il numero unico (UID) viene memorizzato in forma criptata sul dispositivo di memorizzazione dei supporti. L'UID viene riconosciuto come valido solo se i dati dei supporti utente corrispondono.

MIFARE UID
Questo livello di sicurezza è adatto soprattutto alle applicazioni organizzative.

I supporti MIFARE sono conformi allo standard ISO 14443A. Questo definisce che il numero unico (UID) può essere letto senza una chiave aggiuntiva. In questo livello di sicurezza, per l'identificazione viene utilizzato solo l'UID del transponder.

5.5 Sicurezza con le abilitazioni CardLink MIFARE

Chiave impianto
Utilizzando un'autorizzazione CardLink o un Master T, risulta necessaria una chiave impianto (sitekey).

Ogni componente elettronico e il lettore da tavolo sono dotati di hardware di sicurezza speciali che funzionano con questa chiave impianto. Per poter integrare questa chiave specifica nell'impianto di chiusura, è necessaria la tessera di sicurezza C dell'impianto corrispondente. Questa tessera di sicurezza trasmette la chiave impianto all'impianto di chiusura corrispondente. Per ogni impianto di chiusura è necessario impiegare una tessera di sicurezza personalizzata.

Utilizzando una chiave impianto, occorre inizializzare il software di sistema, il lettore da tavolo e i supporti di programmazione corrispondenti. Successivamente la tessera di sicurezza deve essere conservata in un luogo sicuro (es. una cassaforte).

5.6 Sicurezza con l'autorizzazione della whitelist MIFARE

Card ID (CID)
Al posto dell'UID, il sistema assegna un CID personalizzato ai supporti. Tale CID viene crittografato con una chiave impianto personalizzata e scritto nella memoria del supporto. La chiave impianto viene definita da una tessera di sicurezza C.

La tessera di sicurezza C può essere acquistata tramite il canale di distribuzione. Con questa tessera di sicurezza, i componenti elettronici vengono inizializzati con la chiave individuale dell'impianto. Per ogni impianto è necessario impiegare una tessera di sicurezza personalizzata.

Utilizzando una chiave impianto, occorre inizializzare il software di sistema, il lettore da tavolo e i supporti di programmazione corrispondenti. Successivamente la tessera di sicurezza deve essere conservata in un luogo sicuro (es. una cassaforte).

Safe UID
Il livello di sicurezza Safe UID si adatta ad applicazioni con elevati requisiti di sicurezza.

Prerequisito per l'utilizzo della Safe UID è l'applicazione Kaba KCA nei supporti utente. Nella Safe UID, l'UID (numero unico) dei supporti viene ulteriormente verificato nelle memorie dei supporti con un'applicazione speciale. La sicurezza di un UID viene sensibilmente migliorata, poiché il contenuto dell'applicazione non è liberamente accessibile ed è crittografato.

MIFARE UID (conforme a ISO 14443A)
Nella Whitelist è possibile programmare un'autorizzazione con l'UID (numero unico).

Se l'UID corrisponde allo standard ISO 14443A, è possibile registrarlo nella Whitelist. Lo standard ISO prevede la lettura libera dell'UID senza doverlo ulteriormente proteggere. L'utilizzo di tale livello di sicurezza è consigliabile solo per applicazioni organizzative con un requisito di sicurezza minore.

5.7 Master T

Il Master T è un tipo speciale di supporto master per componenti standalone. I Master T impiegati in un impianto di chiusura sono validi solo per un determinato periodo e dispongono di funzioni limitate. Questo consente un'elevata flessibilità nella gestione degli impianti di chiusura, in quanto un Master T può essere rilasciato al personale di servizio senza dover ricorrere al Master A o B rilevante in termini di sicurezza.



Un Master T può essere impiegato solo se i componenti sono stati precedentemente configurati con un Master B e il Programmer 1460.

Master T per LEGIC:
Il software di sistema consente di definire supporti Master T per LEGIC. Un Master T viene generato tramite la tessera di sicurezza e può essere utilizzato solo come Master T.

Master T per MIFARE:
Il software di sistema consente di definire supporti Master T per MIFARE. Un Master T può essere generato tramite la tessera di sicurezza C.

I supporti Master T per LEGIC e MIFARE possiedono le seguenti proprietà:

- Applicazione in entrambi i tipi di autorizzazione: CardLink e Whitelist.
- Aggiornamento dei componenti (i componenti devono essere configurati).
- Impostazione dell'orologio dei componenti.
- Lettura del Traceback.
- Periodo di validità limitato.

6 Componenti

I componenti evolo offrono una vasta gamma di funzioni, riassunte nella seguente panoramica. Per le aree rilevanti per la sicurezza sono disponibili componenti con protezione rinforzata meccanicamente. I dettagli sono riportati nelle istruzioni per l'uso separate e nel catalogo dei prodotti.

6.1 Dimensioni di memoria

Di seguito vengono riportate le capacità disponibili per la memoria riscrivibile dei supporti utente:

	MIFARE		LEGIC
Autorizzazioni	**classic**	**DESFire**	**advant**
	in Byte	in Byte	in Byte
Capacità memoria dei supporti utente	1 k	8 k	4 k
Supporti utente CTC	—		3 k
Capacità di memoria delle applicazioni standard	288	744	848
Kaba Common Application (KCA) Safe UID	48	32	—
CardLink (192 byte di dati di utilizzo)	216	192	216
Numero massimo di autorizzazioni su un supporto utente:			
Massimo 512 gruppi di porte configurati:	– fino a 39 diritti individuali – fino a 11 prenotazioni		
Senza gruppi porte:	– fino a 60 diritti individuali – fino a 18 prenotazioni		
Voci di stato:			
Stato dei componenti (32 byte di dati di utilizzo)	48	32	56
Identificazione (32 byte di dati di utilizzo)	48	32	64
Traceback (60 voci)	—	488	512

6.2 Dati tecnici

Supporti utente
Tessere

Designazione	**Valori**
Colori (layout di stampa)	• dormakaba (rosso o blu) • design personalizzato
Condizioni ambientali	
Grado di protezione	IP66 Resiste al bagnato, ma non all'immersione in acqua. Ad esempio, l'uso come chiave per piscina non è consigliato.
Temperatura	-25 ... +70 °C
Umidità dell'aria	0 ... 95% UR, senza condensa
Capacità di memoria dei supporti	

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)



Le tessere sono protette contro hacking e clonazione.

Portachiavi

Designazione	**Valori**
Colori	Blu, nero, rosso, bianco
Condizioni ambientali	
Grado di protezione	IP65
Temperatura	-20 ... +55 °C
Umidità dell'aria	0 ... 95% UR, senza condensa
Capacità di memoria dei supporti	
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)

Chiave con clip

Designazione	**Valori**
Clip	
Colori	
Inserti colorati della clip	Nero, argento, viola, giallo, verde, rosso, blu
Condizioni ambientali	
Grado di protezione	IP67 Resiste all'immersione temporanea in acqua.
Temperatura	-20 ... +70 °C
Umidità dell'aria	0 ... 95% UR, senza condensa
Capacità di memoria dei supporti	
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)
Chiave	
Sistemi di chiusura meccanici	
dormakaba eco	
dormakaba expert	
dormakaba gemini	
dormakaba matrix	
dormakaba penta	
dormakaba quattro	
dormakaba pextra	
dormakaba AP2000	

Kaba star
Kaba star cross
Kaba 20

Supporti utente TouchGo
Portachiavi

Designazione	**Valori**
Colori	
Supporti utente	Nero, bianco
Dimensioni	
L x A x P	36 x 60 x 12 mm
Alimentazione	
Batteria	3V CR2450 litio
Condizioni ambientali	
Grado di protezione	IP 53
Temperatura	-25 ... +65 °C
Umidità dell'aria	0 ... 95% UR, senza condensa
Capacità di memoria dei supporti	
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)

Braccialetto

Designazione	**Valori**
Colori	Grigio
Dimensioni	
L x A x P	56 x 53 x 17 mm
Alimentazione	
Batteria	3V CR2450 litio
Condizioni ambientali	
Grado di protezione	IP67 (impermeabile)
Temperatura	-25 ... +65 °C
Umidità dell'aria	0 ... 95% UR, senza condensa
Capacità di memoria dei supporti	
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)

Porta-schede

Designazione	**Valori**
Colori	
Porta-schede	Nero, argento-nero
Dimensioni	

L x A x P	90 x 58 x 14 mm
Alimentazione	
Batteria	3V CR2430 litio
Condizioni ambientali	
Grado di protezione	IP 53
Temperatura	-25 ... +65 °C
Umidità dell'aria	0 ... 95% UR, senza condensa
Capacità di memoria dei supporti	
H-BE-TGO	a seconda del supporto inserito.

6.3 Supporti master

2 diversi tipi di supporti master, master A e master B, consentono di impostare i componenti sulla modalità di programmazione ( ). Questi supporti vengono impiegati esclusivamente per la concessione dell'autorizzazione e non posseggono di per sé alcuna autorizzazione di accesso.

Supporti master	MIFARE	LEGIC	Funzioni
Master A 	✓	✓	– Master di un impianto con struttura master A/B – I componenti passano alla modalità di programmazione con il master B – Programmazione di componenti con master B
Master B 	✓	✓	– Master di un impianto – I componenti passano alla modalità di programmazione – Programmazione di componenti con supporti utente
Master T 	✓	✓	– Master T per l'aggiornamento di componenti – Valido solo per un tempo limitato – Funzioni limitate
RCID Master B 			RCID Solo TouchGo E110 – Master di un impianto – I componenti passano alla modalità di programmazione – Programmazione di componenti con supporti utente

6.4 Tessere di sicurezza

Le tessere di sicurezza vengono utilizzate in un ambiente LEGIC o MIFARE. Le funzioni delle tessere di sicurezza variano a seconda della tecnologia di cui si avvalgono.

Per LEGIC esistono diverse tessere di sicurezza:

- Tessera di sicurezza C1 per la segmentazione specifica dell'impianto dei supporti
- Tessera di sicurezza C2 per l'inizializzazione dell'impianto mediante lettore da tavolo e componenti di convalida in CardLink

In ambiente MIFARE è possibile impiegare la tessera di sicurezza C:

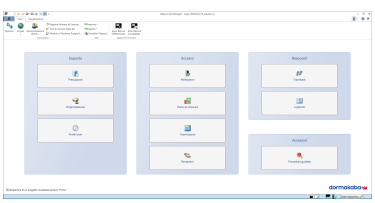
Per poter integrare nell'impianto di chiusura la chiave specifica dell'impianto di un ambiente MIFARE, occorre la tessera di sicurezza C, che definisce la chiave impianto nonché l'organizzazione della memoria dei supporti utente

Tessere di sicurezza	MIFARE	LEGIC	Funzioni
Tessera di sicurezza C 	✓	—	– Definizione chiave impianto (sitekey) – Configurazione supporti – Inizializzazione sistema – Scrittura di applicazioni su tessere vuote.
Scheda di sicurezza C1 (IAM) 	—	✓	– Definizione dello stamp – Inizializzazione sistema – Configurazione supporti – Creazione dei segmenti
Tessera di sicurezza C2 (SAM) 	—	✓	– Definizione dello stamp – Inizializzazione sistema – Autorizzazione di scrittura per lettore da tavolo e componente di convalida – Descrizione dei segmenti.

Autorizzazione di scrittura con la tessera di sicurezza C2
Con la tessera di sicurezza C2, i componenti che devono scrivere i dati nei segmenti sui supporti utente devono ricevere un'autorizzazione di scrittura. Si tratta, ad es., del lettore da tavolo o dei componenti di convalida. Per la descrizione dell'applicazione vedere il capitolo Segnalazioni di applicazione della tessera di sicurezza C2 [▸ 8.5].

6.5 Catena degli strumenti

Una catena degli strumenti comprende gli strumenti di programmazione utilizzati nel sottosistema. Gli strumenti dispongono di svariate funzioni per la configurazione, la gestione, la lettura e la scrittura di componenti e supporti.

Strumento	Funzioni
Programmer 1460 	• Configurazione delle proprietà dei componenti. • Programmazione di componenti. • Lettura del Traceback di componenti. • Aggiornamenti firmware sui componenti. • Messa in funzione di componenti wireless.
Software di sistema: ad es. dormakaba evolo Manager (KEM). 	• Gestione delle autorizzazioni. • Gestione di supporti e persone. • Gestione degli impianti di chiusura. • Valutazione dei dati di traceback.

Strumento	Funzioni
Lettore da tavolo 91 08 	• Lettura e scrittura di supporti. • Organizzazione della memoria del supporto.
Wireless Gateway 90 40-K7 	• Configurazione delle proprietà dei componenti. • Programmazione di componenti. • Lettura del Traceback di componenti. • Aggiornamenti firmware sui componenti.
Wireless Extender 90 41 	• Ampliamento della copertura radio del wireless gateway. • Per componenti wireless.
Ampliamento wireless per lettore remoto 	91 15 + 90 43 • Collegamento wireless per lettori remoti. • Aggiornamento CardLink tramite wireless.
Mobile Access 	Mobile Access • Gestione/accesso tramite smartphone con Bluetooth o NFC.

7 Programmazione / configurazione del componente

Prima della programmazione occorre determinare la tecnologia dei supporti. Si veda il capitolo Determinazione della tecnologia dei supporti [▶ 7.1].

Con la successiva programmazione/configurazione dei componenti sono assegnati i diritti di accesso ed altri diritti.

- I componenti wireless richiedono una messa in funzione wireless prima del primo utilizzo. Vedere la documentazione wireless

7.1 Determinazione della tecnologia dei supporti

Per i componenti Multi RFID (MRD) viene determinata la tecnologia con la quali essi vengono gestiti al momento del primo utilizzo con un Master LEGIC o MIFARE. I componenti, successivamente, si comportano come definito per le tipologie di autorizzazioni LEGIC (LEA) o MIFARE (MID).

Procedura

- Tenere il mastermedium per ca. 1 s davanti all'antenna.
  - La tecnologia del mastermedium (Legic o MIFARE) è stata trasmessa al dispositivo.

Nota: La tecnologia, a seguito di un reset INI, deve essere nuovamente fissata.

7.2 Metodi di programmazione e configurazione

Metodi:

- Senza sistema host con supporti master e utente,
  si veda il capitolo Programmare con i supporti [▶ 7.4]
- con software del sistema e Programmer,
  si veda il capitolo Programmazione con software del sistema e Programmer [▶ 7.5.2]
- Prodotti TouchGo:
  vedi capitolo Programmazione prodotti TouchGo
- Applicazioni wireless:
  messa in funzione con software del sistema e Programmer,
  successivamente viene effettuata la configurazione via gateway wireless,
  si veda il manuale per Programmer, gateway wireless e descrizione del sistema
- Dispositivi di Mobile Access: Dopo la trasmissione della configurazione con il Programmer: inizializzare il dispositivo per il Mobile Access,
  si veda il capitolo Inizializzazione del dispositivo per il Mobile Access [▶ 7.6.2].
- evolo smart:
  L'app guida l'utente attraverso la procedura.

7.3 Programmare i prodotti TouchGo

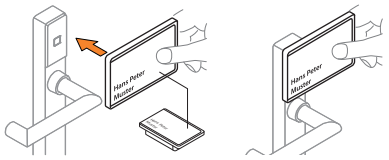
Nel caso di TouchGo, l'autorizzazione di accesso viene verificata al momento del contatto con i componenti.

Prodotto	
c-lever pro TouchGo E110	solo RCID; whitelist standalone Si vedano le istruzioni per l'uso di dormakaba c-lever pro TouchGo
c-lever pro TouchGo E310	RFID e RCID; sottosistema evolo Vedi capitolo Programmare TouchGo E310.

7.3.1 Programmare TouchGo E310

Per la programmazione di TouchGo E310 si utilizzano supporti RFID. Per attivare correttamente la funzione TouchGo, dopo la programmazione è necessario eseguire un accoppiamento dei supporti utente RFID e RCID.

Utilizzare i supporti master e i supporti utente di TouchGo E310 nel modo seguente:



Tenere i supporti master RFID e i supporti combinati (supporti utente RCID/RFID) di TouchGo E310 presso l'antenna RFID (anello luminoso).

7.3.1.1 Programmazione Whitelist manuale

7.3.1.1.1 Programmazione di supporti utente

Dopo l'esposizione del master B, il componente riceve il seguente diritto temporaneo:

- Assegnare al supporto utente presentato l'autorizzazione di accesso (inserire nella white-list).

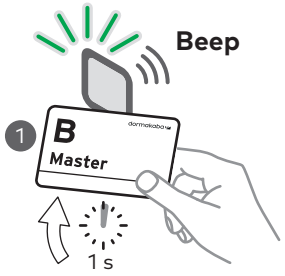
Dopo una successiva presentazione del master B o dopo 20 s senza presentazione di un supporto, al componente viene nuovamente revocato il diritto temporaneo.

Requisiti preliminari

- La struttura A/B oppure
- la struttura B è disponibile

Procedura:

1. Tenere il master B circa **1 s** davanti all'antenna.



   ⇨ luce verde accesa.

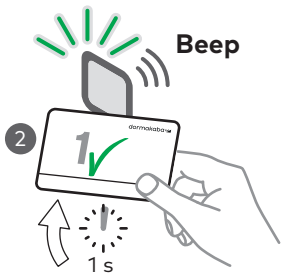
   ⇨ 1 bip breve.

   ⇨ la luce verde si spegne.

Se per 20 s non viene presentato nessun supporto, la procedura termina automaticamente:

-> Le modifiche sono state acquisite e viene emesso 1 segnale acustico lungo.

2. Tenere il supporto utente per ca. **1 s** davanti all'antenna.



   ⇨ luce verde accesa.

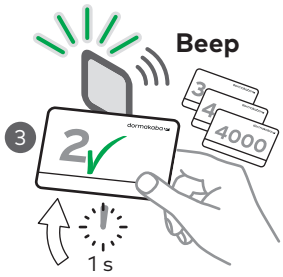
   ⇨ 1 bip breve.

⇨ la luce verde si spegne.

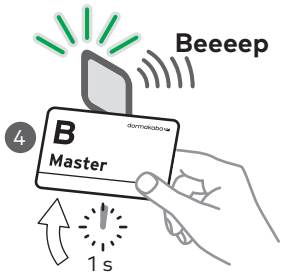
⇨ Il supporto utente è stato inserito nella whitelist .

⇨ Il supporto utente ha accesso al componente.

Programmazione di altri supporti utente: Ripetere il passaggio 2.



3. Tenere il master B circa 1 s davanti all'antenna.



⇨ luce verde accesa.

⇨ 1 bip lungo.

⇨ la luce verde si spegne.

⇨ Le modifiche sono state acquisite.

⇨ La programmazione è terminata.

Se necessario, assegnare autorizzazioni di accesso con altri master B.

7.3.1.1.2 Annullare singola autorizzazione

Annullare l'autorizzazione di accesso di un supporto utente.

Dopo l'esposizione del master B, il componente riceve il seguente diritto temporaneo:

- Revocare l'autorizzazione di accesso al supporto utente presentato (rimuovere dalla whitelist).

Presentando nuovamente il master B, al componente viene revocato il diritto temporaneo.

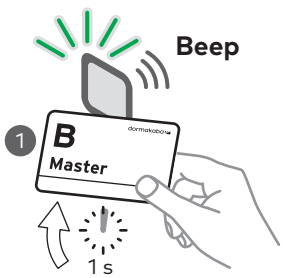
Requisiti preliminari

- Supporto utente con autorizzazione di accesso.
- La struttura A/B oppure
- la struttura B è disponibile

Procedura

All'occorrenza, presentare altri supporti utente.

1. Tenere il master B circa **1 s** davanti all'antenna.

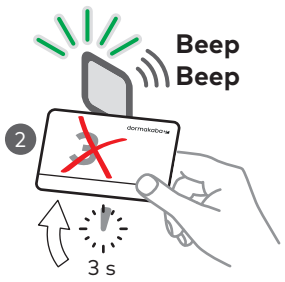


⇨ luce verde accesa.
⇨ 1 bip breve.
⇨ la luce verde si spegne.

Se per 20 s non viene presentato nessun supporto, la procedura termina automaticamente:

-> Le modifiche sono state acquisite e viene emesso 1 segnale acustico lungo.

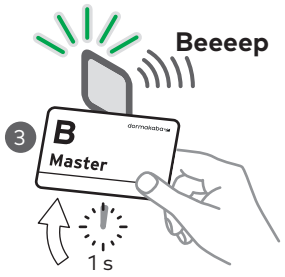
2. Tenere il supporto utente per ca. **3 s** davanti all'antenna.



⇨ luce verde accesa.
⇨ Sono emessi 2 segnali acustici brevi.
⇨ la luce verde si spegne.
⇨ Il supporto utente è stato rimosso dalla whitelist . Il supporto utente non ha accesso al componente.

All'occorrenza, presentare altri supporti utente.

3. Tenere il master B circa 1 s davanti all'antenna.



⇨ luce verde accesa.
⇨ 1 bip lungo.
⇨ la luce verde si spegne.
⇨ Le modifiche sono state acquisite.

⇨ La procedura è terminata.

7.3.1.1.3 Annullare tutte le autorizzazioni di accesso

Dopo l'esposizione del master B, il componente riceve il seguente diritto temporaneo:

- Annulla tutte le autorizzazioni di accesso assegnate dal master B (rimuovere dalla whitelist).

Nota: Il master B conserva il diritto di assegnare autorizzazioni d'accesso.

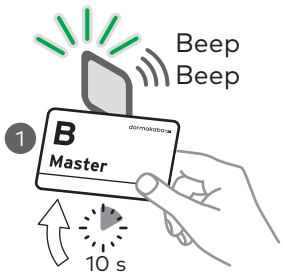
Procedura

AVVISO

Perdita di dati

Se il master B viene esposto per **15 s**, viene effettuato un reset INI.
Il reset INI cancella tutte le impostazioni e i dati salvati nel componente.

1. Tenere il master B circa **10 s** davanti all'antenna.



   ⇨ luce verde accesa.

   ⇨ Dalla versione 42 del firmware: Sono emessi 1 segnale acustico lungo e 2 brevi.
   Prima della versione 42 del firmware: Sono emessi 2 segnali acustici brevi.

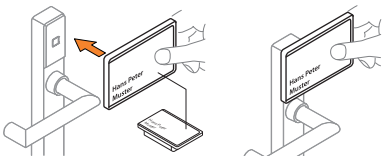
   ⇨ la luce verde si spegne.

   ⇨ Tutti i diritti di accesso assegnati tramite il master B sono stati annullati.

⇨ La procedura è terminata.

7.3.1.2 Accoppiamento RCID/RFID

TouchGo E310 è utilizzato nel sistema evolo di dormakaba. Per la programmazione e l'identificazione viene utilizzata la tecnologia RFID. Per consentire l'efficacia della funzione TouchGo, è necessario un accoppiamento dei supporti utente RFID e RCID.



7.3.1.2.1 Assegnare l'autorizzazione RCID

Autorizzazione Whitelist
L'autorizzazione viene programmata direttamente tramite l'antenna RFID con il supporto master RFID e i supporti combinati (supporti utente RCID/RFID). Durante la lettura del supporto combinato, i dati RFID vengono "sposati" con i dati RCID (TouchGo) nel cosiddetto accoppiamento.

Autorizzazione CardLink
L'autorizzazione viene fornita tramite il software di sistema e applicata direttamente tramite l'antenna RFID con i supporti combinati (supporti utente RFID/RCID). Durante la lettura del supporto combinato, i dati RFID vengono "sposati" con i dati RCID (TouchGo) nel cosiddetto accoppiamento.

Le modifiche future dell'autorizzazione e l'aggiornamento della convalida sono trasferite con la tecnologia RFID sui componenti e contemporaneamente viene verificato l'accoppiamento.

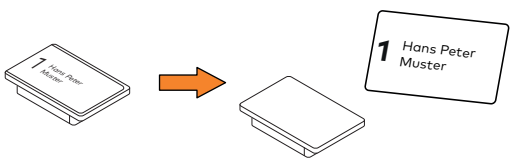
I supporti RCID non possono essere programmati due volte (accoppiamento già presente).

7.3.1.2.2 Annullare autorizzazione RCID

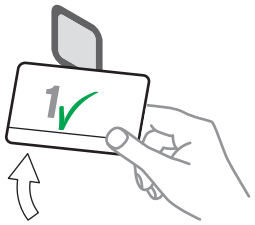
Annullare l'autorizzazione RCID scollegando la coppia RCID/RFID. Ciò non è possibile nei supporti combinati.

Procedura

1. Scollegare fisicamente il supporto RFID e il supporto RCID.
   Ad es., rimuovere la scheda dal porta-schede.



2. Collocare il supporto RCID a circa 2 m di distanza su un altro tavolo.
   ⇨ Non indossare il supporto RCID.
3. Presentare il supporto RFID al componente.



⇨ L'accoppiamento è annullato.

7.3.1.3 Parametrizzare TouchGo E310 nel software di sistema

Negli impianti di chiusura gestiti con un software di sistema, è possibile utilizzare anche componenti TouchGo E310. I supporti combinati (supporti utente RCID/RFID) vengono programmati con un supporto master RFID nei componenti oppure i dati RFID vengono registrati e gestiti con il lettore da tavolo. Le autorizzazioni di accesso del supporto combinato vengono quindi trasferite con il Programmer (autorizzazione whitelist) oppure i dati RFID del supporto combinato (autorizzazione CardLink) sono trasferiti ai componenti.

7.3.1.4 Funzione TimePro

7.3.1.4.1 Modalità di apertura ufficio con whitelist

1 Supporto con TimePro:

L'uso è analogo a quello della modalità di apertura ufficio.
Tramite la funzione TimePro avviene un'attivazione temporizzata.

Numerose registrazioni TimePro:

Attivazione tramite il supporto combinato o la funzione TouchGo (toccare la maniglia interna).
Disattivazione tramite supporto combinato oppure l'arco di tempo impostato.

7.3.1.4.2 Modalità di apertura ufficio con CardLink

Attivare la funzione TimePro oppure la modalità di apertura ufficio tramite il supporto combinato oppure TouchGo (toccare la maniglia interna).
Disattivazione tramite supporto combinato oppure l'arco di tempo impostato.

7.3.1.5 Programmare le autorizzazioni per la modalità di apertura ufficio

La funzione modalità di apertura ufficio TouchGo è illustrata nel capitolo Uso.
Questo capitolo descrive l'assegnazione o la revoca dell'autorizzazione, nonché l'attivazione o la disattivazione della modalità di apertura ufficio.

E310
Le autorizzazioni vengono concesse per mezzo del software di sistema agli utenti.

E110
Programmazione per TouchGo E110:

- Assegnare l'autorizzazione: Capitolo [▸ 7.3.1.5.1]
- Annullare autorizzazione:
  - Autorizzazione singola: Capitolo [▸ 7.3.1.5.2]
  - Tutte le autorizzazioni: Capitolo [▸ 7.3.1.5.3]

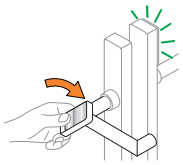
7.3.1.5.1 Assegnare autorizzazione per la modalità di apertura ufficio

- Non stringere in mano il supporto master e il supporto utente.



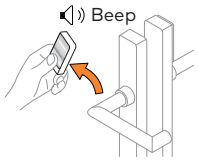
- Tenere in mano 1 solo supporto. Assicurarsi che gli altri supporti si trovino almeno a 2 m di distanza.

1. Tenere in mano il supporto master.
2. Toccare con l'indice la maniglia interna.



⇨ luce verde accesa.

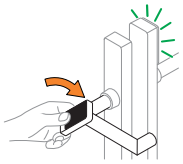
3. Rimuovere l'indice/il supporto master.



⇨ la luce verde si spegne.

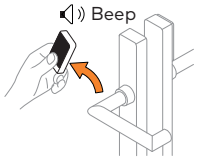
⇨ 1 bip breve.

4. Prendere in mano il supporto utente.
5. Toccare con l'indice la maniglia interna.



⇨ luce verde accesa.

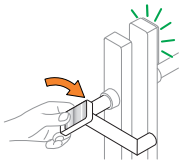
6. Rimuovere l'indice/il supporto utente.



⇨ la luce verde si spegne.

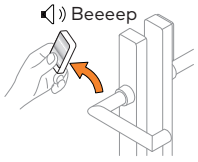
⇨ 1 bip breve.

7. Tenere in mano il supporto master.
8. Toccare con l'indice la maniglia interna.



⇨ luce verde accesa.

9. Rimuovere l'indice/il supporto master.



⇨ la luce verde si spegne.

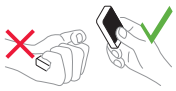
⇨ 1 bip lungo.

⇨ L'autorizzazione di accesso modalità di apertura ufficio è stata assegnata.

7.3.1.5.2 Annullare singola autorizzazione per la modalità di apertura ufficio

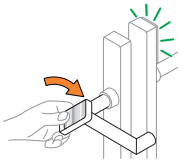
Annullare l'autorizzazione per la modalità di apertura ufficio di un supporto utente.

- Non stringere in mano il supporto master e il supporto utente.



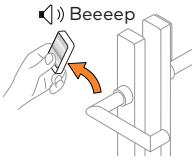
- Tenere in mano 1 solo supporto. Assicurarsi che gli altri supporti si trovino almeno a 2 m di distanza.

1. Tenere in mano il supporto master.
2. Toccare con l'indice la maniglia interna.



⇨ luce verde accesa.

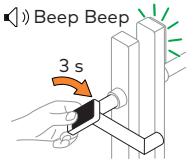
3. Rimuovere l'indice/il supporto.



⇨ la luce verde si spegne.

⇨ 1 bip lungo.

4. Prendere in mano il supporto utente.
5. Toccare con l'indice la maniglia interna per 3 s.

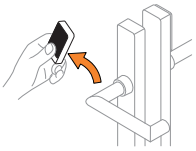


⇨ luce verde accesa.

⇨ Sono emessi 2 segnali acustici brevi.

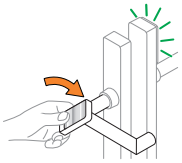
⇨ L'autorizzazione per la modalità di apertura ufficio del supporto è stata annullata.

6. Rimuovere l'indice/il supporto utente.



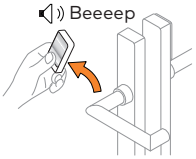
⇨ la luce verde si spegne.

7. Tenere in mano il supporto master.
8. Toccare con l'indice la maniglia interna.



⇨ luce verde accesa.

9. Rimuovere l'indice/il supporto master.



⇨ la luce verde si spegne.

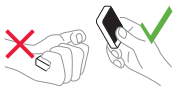
⇨ 1 bip lungo.

⇨ L'autorizzazione per la modalità di apertura ufficio è stata annullata.

7.3.1.5.3 Annullare tutte le autorizzazioni per la modalità di apertura ufficio

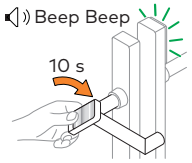
Annullare tutte le autorizzazioni per la modalità di apertura ufficio salvate nei componenti.

- Non stringere in mano il supporto master e il supporto utente.



- Tenere in mano 1 solo supporto. Assicurarsi che gli altri supporti si trovino almeno a 2 m di distanza.

1. Tenere in mano il supporto master.
2. Toccare la maniglia interna per 10 s.

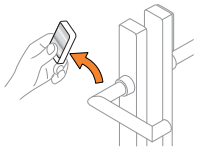


⇨ luce verde accesa.

⇨ Sono emessi 2 segnali acustici brevi.

⇨ Tutte le autorizzazioni sono state annullate.

3. Rimuovere l'indice/il supporto master.



⇨ la luce verde si spegne.

⇨ Tutte le autorizzazioni per la modalità di apertura di ufficio sono state annullate.

7.3.2 Supporti utente persi/guasti

Per la sicurezza dell'impianto è necessario annullare le autorizzazioni dei supporti utente persi oppure guasti. Le autorizzazioni dei supporti utente residui vengono successivamente riprogrammate.

Procedura:

1. Annullare tutte le autorizzazioni. Vedi [▸ 7.3.1.1.3]
   ⇨ Le autorizzazione di accesso vengono annullate.
   ⇨ Le autorizzazioni per la modalità di apertura ufficio vengono annullate.
2. Riprogrammare i supporti utente.
   ⇨ Riprogrammare le autorizzazioni di accesso. Vedi [▸ 7.3.1.1.1]
   ⇨ Programmare di nuovo le autorizzazioni per la modalità di apertura ufficio. Vedi [▸ 7.3.1.5]

7.4 Programmare con i supporti

Tenendo premuto un supporto Master (circa 1 s) si attiva la modalità di programmazione.
Uscire dalla modalità di programmazione:
automaticamente, 20 s dopo la presentazione dell'ultimo supporto (time-out) o
tenendo nuovamente premuto il supporto Master (circa 1 s).

7.4.1 Tessere

7.4.1.1 Definire il supporto Master di livello superiore

- Il supporto Master di livello superiore è il supporto più alto di un componente.
- A ciascun componente deve essere assegnato 1 supporto Master di livello superiore.
- A ciascun componente può essere assegnato solo 1 supporto Master di livello superiore.
- Il primo supporto Master presentato per un componente viene inserito come supporto Master di livello superiore.

Struttura A/B

- In una struttura A/B, il supporto Master di livello superiore deve essere un Master A.
- Un Master A può concedere diritti ai supporti Master B. Vedere il capitolo "Creare una struttura A/B".
- Un Master A può ritirare i diritti dai supporti del Master B. Vedere il capitolo "Cancellare il Master B dal componente".
- Un reset INI può essere avviato sul componente con un Master A, vedere il capitolo "Reset INI con supporto Master".

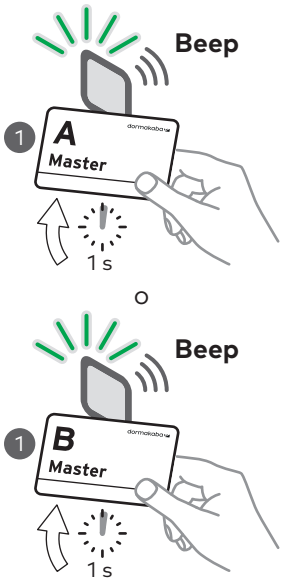
Struttura B

- In una struttura B, il supporto Master di livello superiore deve essere un Master B.
- Un reset INI può essere avviato sul componente con un Master B, vedere il capitolo "Reset INI con supporto Master".

Requisiti preliminari

- Il componente è in stato di consegna, vedi reset INI.

Procedura

	Tenere il supporto Master (A o B) davanti all'antenna per circa **1 s.** -> luce verde accesa. -> viene emesso 1 breve segnale acustico. -> luce verde spenta. -> Il supporto Master presentato è stato inserito come supporto master di livello superiore.	1x breve

7.4.1.2 Creare una struttura A/B

Dopo l'esposizione del Master A, il componente riceve il seguente diritto temporaneo:

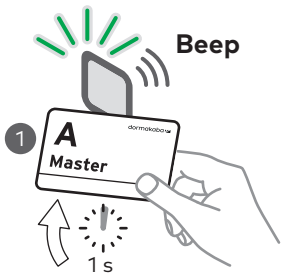
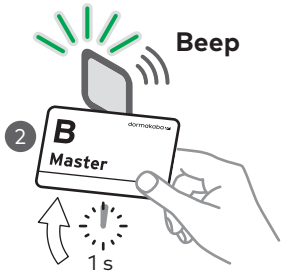
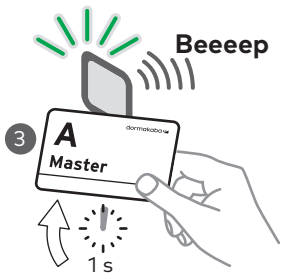
- concedere al Master B presentato il diritto di assegnare i diritti di accesso ai supporti utente.

Presentando nuovamente il Master A, al componente viene revocato di nuovo il diritto temporaneo.

Requisiti preliminari

- Il Master A presentato è il supporto di livello superiore del componente.
  Vedere il capitolo "Definire il supporto Master di livello superiore"

Procedura

	Tenere il Master A davanti all'antenna per circa **1 s.** -> luce verde accesa. -> viene emesso 1 breve segnale acustico. -> luce verde spenta.	1x breve
	Se per 20 s non viene presentato nessun supporto, la procedura termina automaticamente: -> Le modifiche sono state acquisite e viene emesso 1 segnale acustico lungo.	
	Tenere il master B circa **1 s** davanti all'antenna. -> luce verde accesa. -> viene emesso 1 breve segnale acustico. -> luce verde spenta. -> Il Master B ha il diritto di assegnare i diritti di accesso ai supporti utente. -> Viene creata la struttura A/B.	1x breve
	Se necessario, presentare ulteriori Master B.	
	Tenere il Master A davanti all'antenna per circa **1 s.** -> luce verde accesa. -> viene emesso 1 segnale acustico lungo. -> luce verde spenta.	1x lungo

7.4.1.3 Assegnare autorizzazioni di accesso

Dopo l'esposizione del master B, il componente riceve il seguente diritto temporaneo:

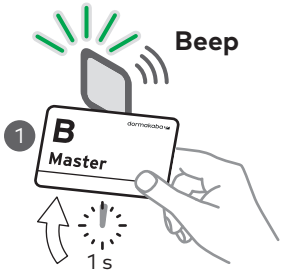
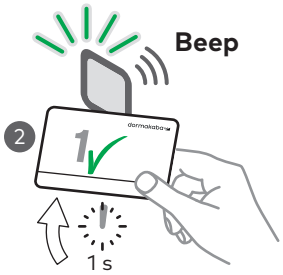
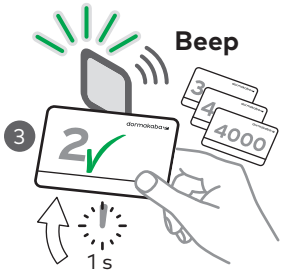
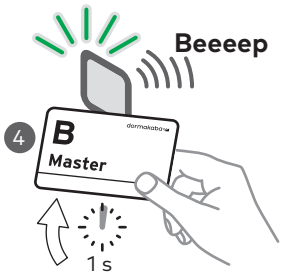
- Assegnare al supporto utente presentato l'autorizzazione di accesso (inserire nella white-list).

Presentando nuovamente il master B, al componente viene revocato il diritto temporaneo.

Requisiti preliminari

- La struttura A/B oppure
- la struttura B è disponibile

Procedura

	Tenere il master B circa **1 s** davanti all'antenna. -> luce verde accesa. -> viene emesso 1 breve segnale acustico. -> luce verde spenta.	1x breve
	Se per 20 s non viene presentato nessun supporto, la procedura termina automaticamente: -> Le modifiche sono state acquisite e viene emesso 1 segnale acustico lungo.	
	Tenere il supporto utente per ca. **1 s** davanti all'antenna. -> luce verde accesa. -> viene emesso 1 breve segnale acustico. -> luce verde spenta. -> Il supporto utente è stato inserito nella whitelist . Il supporto utente ha accesso al componente.	1x breve
	Se necessario, aggiungere altri supporti utente alla whitelist: Ripetere il passaggio 2.	1x breve
	Tenere il master B circa 1 s davanti all'antenna. -> luce verde accesa. -> viene emesso 1 segnale acustico lungo. -> luce verde spenta. -> Le modifiche sono state acquisite.	1x lungo
	Se necessario, assegnare autorizzazioni di accesso con altri master B.	

7.4.1.4 Annullare singole autorizzazioni di accesso

Dopo l'esposizione del master B, il componente riceve il seguente diritto temporaneo:

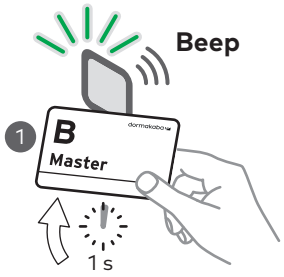
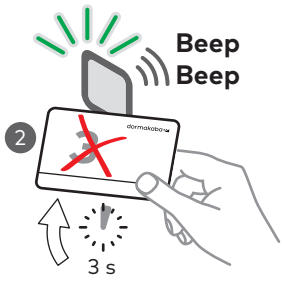
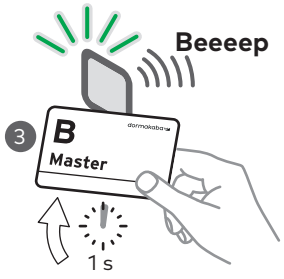
- Revocare l'autorizzazione di accesso al supporto utente presentato (rimuovere dalla whitelist).

Presentando nuovamente il master B, al componente viene revocato il diritto temporaneo.

Requisiti preliminari

- Supporto utente con autorizzazione di accesso.
- La struttura A/B oppure
- la struttura B è disponibile

Procedura

	Tenere il master B circa **1 s** davanti all'antenna. -> luce verde accesa. -> viene emesso 1 breve segnale acustico. -> luce verde spenta.	1x breve
	Se per 20 s non viene presentato nessun supporto, la procedura termina automaticamente: -> Le modifiche sono state acquisite e viene emesso 1 segnale acustico lungo.	
	Tenere il supporto utente per ca. **3 s** davanti all'antenna. -> luce verde accesa. -> sono emessi 2 segnali acustici brevi. -> luce verde spenta. -> Il supporto utente è stato rimosso dalla whitelist . Il supporto utente non ha accesso al componente. All'occorrenza, presentare altri supporti utente.	2x brevi
	Tenere il master B circa 1 s davanti all'antenna. -> luce verde accesa. -> viene emesso 1 segnale acustico lungo. -> luce verde spenta. -> Le modifiche sono state acquisite.	1x lungo

7.4.1.5 Cancellare il Master B dal componente

Una volta che il Master A è disponibile, il componente riceve i seguenti diritti temporanei:

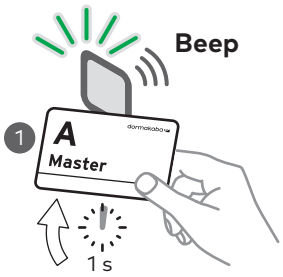
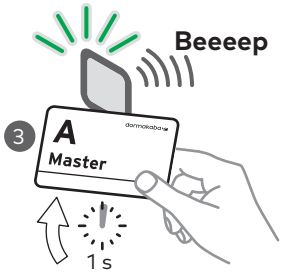
- Annullare tutte le autorizzazioni di accesso assegnate dal Master B presentato (rimuovere dalla whitelist).
- Revocare il diritto di assegnare autorizzazioni di accesso dal Master B presentato.

Dopo che il Master A è stato nuovamente presentato, i diritti temporanei vengono revocati di nuovo dal componente.

Requisiti preliminari

- Il Master B ha ricevuto i suoi diritti attraverso il Master A
- La struttura A/B è disponibile

Procedura

	Tenere il Master A davanti all'antenna per circa **1 s.** -> luce verde accesa. -> viene emesso 1 breve segnale acustico. -> luce verde spenta.	1x breve
	Se per 20 s non viene presentato nessun supporto, la procedura termina automaticamente: -> Le modifiche sono state acquisite e viene emesso 1 segnale acustico lungo.	
	Tenere il Master B davanti all'antenna (circa 10 s) finché non si sentono 2 brevi segnali acustici. -> Il verde si accende finché viene presentato il Master B. Se necessario, presentare ulteriori Master B.	2x brevi
	Tenere il Master A davanti all'antenna per circa **1 s.** -> luce verde accesa. -> viene emesso 1 segnale acustico lungo. -> luce verde spenta. -> Le modifiche sono state acquisite.	1x lungo

7.4.1.6 Annullare tutte le autorizzazioni di accesso assegnate dal Master B

Dopo l'esposizione del master B, il componente riceve il seguente diritto temporaneo:

- Annulla tutte le autorizzazioni di accesso assegnate dal master B (rimuovere dalla whitelist).

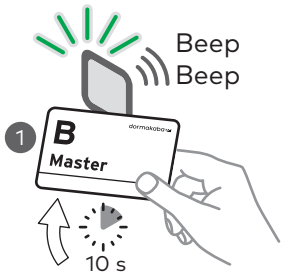
Nota: Il master B conserva il diritto di assegnare autorizzazioni d'accesso.

Procedura

AVVISO

Perdita di dati

Se il master B viene esposto per **15 s**, viene effettuato un reset INI.
Il reset INI cancella tutte le impostazioni e i dati salvati nel componente.

	Tenere il master B circa **10 s** davanti all'antenna. -> luce verde accesa. -> sono emessi 1 segnale lungo e 1 breve (dalla versione del firmware 42). -> (prima della versione 42 del firmware: sono emessi 2 segnali acustici brevi.) -> luce verde spenta. -> Tutti i diritti di accesso assegnati tramite il master B sono stati annullati.	Dalla versione 42 del firmware: 1x lungo 1x breve Prima della versione 42 del firmware: 2x brevi

7.4.2 Chiave

7.4.2.1 Definire il supporto Master di livello superiore

- Il supporto Master di livello superiore è il supporto più alto di un componente.
- A ciascun componente deve essere assegnato 1 supporto Master di livello superiore.
- A ciascun componente può essere assegnato solo 1 supporto Master di livello superiore.
- Il primo supporto Master inserito nel cilindro viene inserito come supporto Master di livello superiore.

Struttura A/B

- In una struttura A/B, il supporto Master di livello superiore deve essere un Master A.
- Un Master A può concedere diritti ai supporti Master B. Vedere il capitolo "Creare una struttura A/B".
- Un Master A può ritirare i diritti dai supporti del Master B. Vedere il capitolo "Cancellare il Master B dal componente".
- Un reset INI può essere avviato sul componente con un Master A, vedere il capitolo "Reset INI con supporto Master".

Struttura B

- In una struttura B, il supporto Master di livello superiore deve essere un Master B.
- Un reset INI può essere avviato sul componente con un Master B, vedere il capitolo "Reset INI con supporti Master".

Requisiti preliminari

- Il componente è in stato di consegna, vedi reset INI.

Procedura

Master A Beep 1 1 s o Master B Beep 1 1 s	Inserire il supporto Master (A o B) nel cilindro per circa **1 s.** -> viene emesso 1 breve segnale acustico. -> Il supporto Master presentato è stato inserito come supporto master di livello superiore.	1x breve

7.4.2.2 Creare una struttura A/B

Dopo l'inserimento del Master A, il componente riceve il seguente diritto temporaneo:

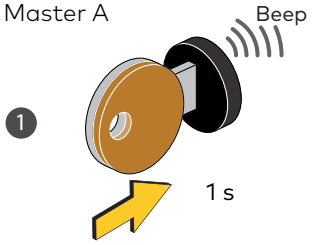
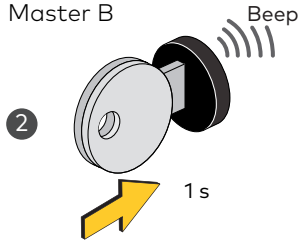
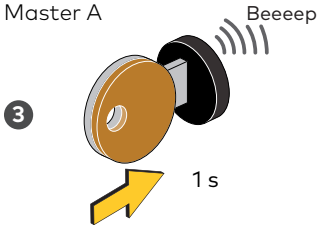
- Autorizzare il Master-B inserito nel cilindro ad assegnare i diritti di accesso ai supporti utente.

Inserendo nuovamente il Master A, al componente viene revocato di nuovo il diritto temporaneo.

Requisiti preliminari

- Il Master-A inserito nel cilindro è il supporto di livello superiore del componente. Vedere il capitolo "Definire il supporto Master di livello superiore"

Procedura

Master A Beep  	Inserire il Master A per circa **1 s** nel cilindro. -> viene emesso 1 breve segnale acustico.	1x breve
	Se non viene inserito nessun supporto nel cilindro per 20 secondi, il processo si conclude automaticamente: -> Le modifiche sono state acquisite e viene emesso 1 segnale acustico lungo.	
Master B Beep  	Inserire il Master B per circa **1 s** nel cilindro. -> viene emesso 1 breve segnale acustico. -> Il Master B ha il diritto di assegnare i diritti di accesso ai supporti utente. -> Viene creata la struttura A/B.	1x breve
	Se necessario, presentare ulteriori Master B.	
Master A Beeeep  	Inserire il Master A per circa **1 s** nel cilindro. -> viene emesso 1 segnale acustico lungo.	1x lungo

7.4.2.3 Assegnare autorizzazioni di accesso

Dopo l'inserimento del master B, il componente riceve il seguente diritto temporaneo:

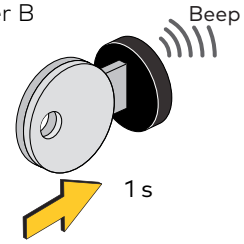
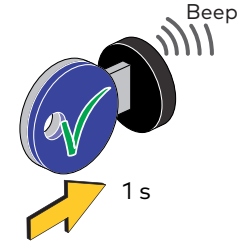
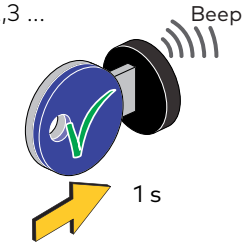
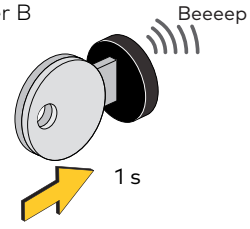
- Assegnare l'autorizzazione di accesso al supporto utente inserito nel cilindro (inserire nella whitelist).

Inserendo nuovamente il Master B, al componente viene revocato di nuovo il diritto temporaneo.

Requisiti preliminari

- La struttura A/B oppure
- la struttura B è disponibile

Procedura

Master B Beep 1 	Inserire il Master B per circa **1 s** nel cilindro. -> viene emesso 1 breve segnale acustico.	1x breve
	Se non viene inserito nessun supporto nel cilindro per 20 secondi, il processo si conclude automaticamente: -> Le modifiche sono state acquisite e viene emesso 1 segnale acustico lungo.	
User 1 Beep 2 	Inserire il supporto utente nel cilindro per circa **1 s.** -> viene emesso 1 breve segnale acustico. -> Il supporto utente è stato inserito nella whitelist . Il supporto utente ha accesso al componente.	1x breve
User 2,3 ... Beep 3 	Se necessario, aggiungere altri supporti utente alla whitelist: Ripetere il passaggio 2.	1x breve
Master B Beeeep 4 	Inserire il Master B per circa 1 s nel cilindro. -> viene emesso 1 segnale acustico lungo. -> Le modifiche sono state acquisite.	1x lungo
	Se necessario, assegnare autorizzazioni di accesso con altri master B.	

7.4.2.4 Annullare singole autorizzazioni di accesso

Dopo l'inserimento del master B, il componente riceve il seguente diritto temporaneo:

- Revoca dell'autorizzazione di accesso al supporto utente inserito nel cilindro (rimuovere dalla whitelist).

Inserendo nuovamente il Master B, al componente viene revocato di nuovo il diritto temporaneo.

Requisiti preliminari

- Supporto utente con autorizzazione di accesso.
- La struttura A/B oppure
- la struttura B è disponibile

Procedura

Master B Beep 1 1 s	Inserire il Master B per circa **1 s** nel cilindro. -> viene emesso 1 breve segnale acustico.	1x breve
	Se non viene inserito nessun supporto nel cilindro per 20 secondi, il processo si conclude automaticamente: -> Le modifiche sono state acquisite e viene emesso 1 segnale acustico lungo.	
User Beep Beep 2 3 s	Inserire il supporto utente nel cilindro per circa **3 s.** -> vengono emessi 2 segnali acustici brevi. -> Il supporto utente è stato rimosso dalla whitelist . Il supporto utente non ha accesso al componente. All'occorrenza, presentare altri supporti utente.	2x brevi
Master B Beeeep 3 1 s	Inserire il Master B per circa 1 s nel cilindro. -> viene emesso 1 segnale acustico lungo. -> Le modifiche sono state acquisite.	1x lungo

7.4.2.5 Cancellare il Master B dal componente

Dopo aver inserito il Master A, il componente riceve i seguenti diritti temporanei:

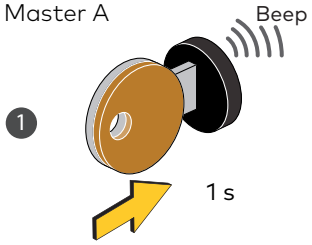
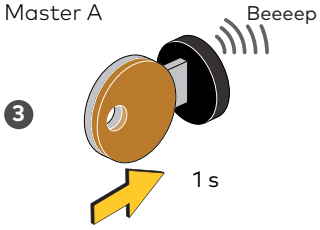
- Annullare tutte le autorizzazioni di accesso assegnate dal master B inserito (rimuovere dalla whitelist).
- Revocare il diritto di assegnare autorizzazioni di accesso dal Master B inserito.

Dopo che il Master A è stato nuovamente inserito, i diritti temporanei vengono revocati di nuovo dal componente.

Requisiti preliminari

- Il Master B ha ricevuto i suoi diritti attraverso il Master A
- La struttura A/B è disponibile

Procedura

Master A Beep  	Inserire il Master A per circa **1 s** nel cilindro. -> viene emesso 1 breve segnale acustico.	1x breve
	Se non viene inserito nessun supporto nel cilindro per 20 secondi, il processo si conclude automaticamente: -> Le modifiche sono state acquisite e viene emesso 1 segnale acustico lungo.	
Master B Beep Beep  	Inserire il Master B nel cilindro (circa 10 s) fino all'emissione di 2 brevi segnali acustici. Se necessario, presentare ulteriori Master B.	2x brevi
Master A Beeeep  	Inserire il Master A per circa **1 s** nel cilindro. -> viene emesso 1 segnale acustico lungo. -> Le modifiche sono state acquisite.	1x lungo

7.4.2.6 Annullare tutte le autorizzazioni di accesso assegnate dal Master B

Dopo l'inserimento del master B, il componente riceve il seguente diritto temporaneo:

- Annulla tutte le autorizzazioni di accesso assegnate dal master B (rimuovere dalla whitelist).

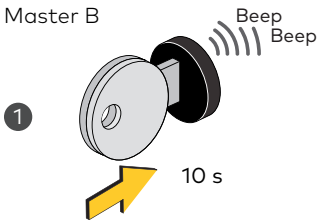
Nota: Il master B conserva il diritto di assegnare autorizzazioni d'accesso.

Procedura

AVVISO

Perdita di dati

Se il Master-B è inserito per **15 s**, inizia il reset INI.
Il reset INI cancella tutte le impostazioni e i dati salvati nel componente.

	Inserire il Master B per circa **10 s** nel cilindro. -> sono emessi 1 segnale lungo e 2 brevi (dalla versione del firmware 42). -> (prima della versione 42 del firmware: sono emessi 2 segnali acustici brevi). -> Tutti i diritti di accesso assegnati tramite il master B sono stati annullati.	Dalla versione 42 del firmware: 1x lungo 1x breve Prima della versione 42 del firmware: 2x brevi

7.4.3 Reset INI con supporti master

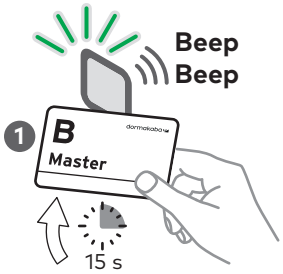
Effetti del reset INI

- Le parametrizzazioni e i dati vengono cancellati e ripristinati ai valori originari (impostazione di fabbrica).
- Durante il reset INI il punto di accesso è bloccato.
- Tutte le autorizzazioni di accesso, i supporti Master e il Traceback vengono cancellati.
- Il punto di accesso è bloccato dopo il reset INI.

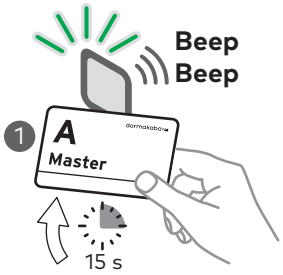
7.4.3.1 Tessere

7.4.3.1.1 Whitelist

Nella struttura Master B

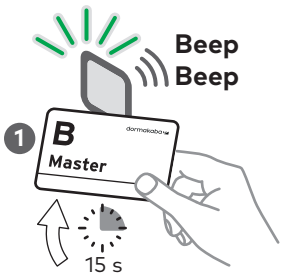
Reset INI con Master B		
	Tenere il Master B circa **15 s** davanti all'antenna. -> luce verde accesa. -> Si emettono segnali acustici. -> Il reset INI viene eseguito dopo 15 secondi. -> luce verde spenta.	dopo 10 s: 1x lungo, 1x brevemente, dopo 15 s, 2x brevi

Nella struttura Master A/B

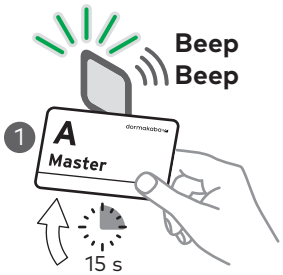
Reset INI con Master A		
	Tenere il Master A circa **15 s** davanti all'antenna. -> luce verde accesa. -> Si emettono segnali acustici. -> Il reset INI viene eseguito dopo 15 secondi. -> luce verde spenta.	dopo 10 s: 1x lungo, 1x brevemente, dopo 15 s, 2x brevi

7.4.3.1.2 CardLink

Con Master B

Reset INI con Master B		
	Tenere il Master B circa **15 s** davanti all'antenna. -> luce verde accesa. -> Il reset INI viene eseguito dopo 15 secondi. -> sono emessi 2 segnali acustici brevi. -> luce verde spenta.	2x brevi

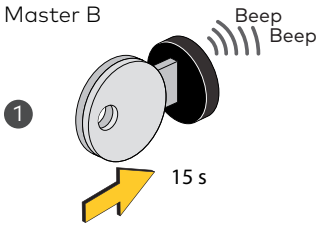
Con Master A

Reset INI con Master A		
	Tenere il Master A circa **15 s** davanti all'antenna. -> luce verde accesa. -> Il reset INI viene eseguito dopo 15 secondi. -> sono emessi 2 segnali acustici brevi. -> luce verde spenta.	2x brevi

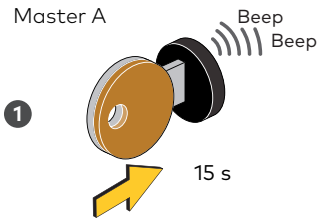
7.4.3.2 Chiave

7.4.3.2.1 Whitelist

Nella struttura Master B

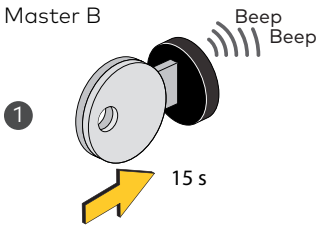
Reset INI con Master B		
	Inserire il Master B per circa **15 s** nel cilindro. -> Si emettono segnali acustici. -> Il reset INI viene eseguito dopo 15 secondi.	dopo 10 s: 1x lungo, 1x brevemente, dopo 15 s, 2x brevi

Nella struttura Master A/B

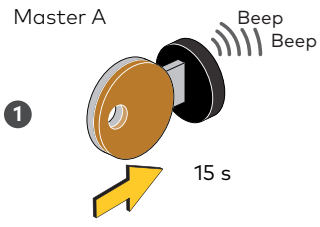
Reset INI con Master A		
	Inserire il Master A per circa **15 s** nel cilindro. -> Si emettono segnali acustici. -> Il reset INI viene eseguito dopo 15 secondi.	dopo 10 s: 1x lungo, 1x brevemente, dopo 15 s, 2x brevi

7.4.3.2.2 CardLink

Con Master B

Reset INI con Master B		
	Inserire il Master B per circa **15 s** nel cilindro. -> Il reset INI viene eseguito dopo 15 secondi. -> sono emessi 2 segnali acustici brevi.	2x brevi

Con Master A

Reset INI con Master A		
	Inserire il Master A per circa **15 s** nel cilindro. -> Il reset INI viene eseguito dopo 15 secondi. -> sono emessi 2 segnali acustici brevi.	2x brevi

7.5 Programmazione con il software di sistema

Questo tipo di programmazione consente di trasmettere i dati configurati nel software di sistema sui componenti con il programmer o tramite wireless. Per questo tipo di programmazione sono obbligatori i supporti master dell'impianto di chiusura. Nel caso di funzionamento wireless, i supporti master sono necessari per la messa in funzione dei componenti. La programmazione di funzioni di temporizzazione e la lettura del Traceback (memoria di eventi) sono possibili con questo tipo di programmazione.

Con il software di sistema sono gestiti componenti e supporti e assegnate le autorizzazioni. È possibile visualizzare un'ampia gamma di dati organizzativi, costruttivi e personali e tenere traccia di tutti i movimenti.

7.5.1 Software di sistema per componenti evolo

In base al campo d'impiego e alla grandezza dell'impianto sono utilizzati diversi software di sistema.

7.5.2 Programmazione con software del sistema e Programmer

Procedura

- Configurare il dispositivo nel software del sistema.
- Trasmettere la configurazione sul Programmer.
- Tenere il mastermedium per ca. 1 s davanti all'antenna.
- Collegare il Programmer al dispositivo.
- Trasferire la configurazione dal Programmer al dispositivo.

Si veda anche:

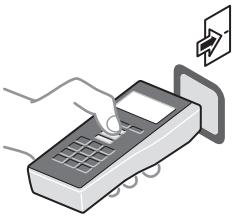
- descrizione del sistema
- Documentazione del software di sistema usato
- Istruzioni per l'uso Programmer 1460
- Linea guida di pianificazione wireless

7.5.3 Esportazione in componenti

Durante l'esportazione, i dati di configurazione vengono trasferiti dal Programmer ai componenti.

Per l'esportazione, i dati di configurazione dei piani di chiusura devono prima essere trasferiti dal software di sistema al Programmer.

7.5.3.1 Esporta in componenti evolo



Selezionare i dati di configurazione sulla lista nel programmer ed esportarli nei componenti.

✓ Supporto master valido disponibile

1. Premere il tasto menu Esporta.
   ⇨ Apertura del menu Esporta.
2. Accedere al componente tramite master.

Attivare l'elettronica della serratura per armadietti 21 10 premendo brevemente la porta.

3. Selezionare il piano di chiusura.
4. Premere il tasto INVIO.
5. Selezionare l'attuatore.
6. Premere il tasto INVIO.

7.5.4 Importazione da componenti

Attivare l'elettronica della serratura per armadietti 21 10 premendo brevemente la porta.

Durante l'importazione i dati di configurazione vengono trasmessi dai componenti al Programmer. Successivamente, il Programmer viene collegato ad un PC per elaborare ulteriormente i dati con un sistema host, ad es. nell'analisi traceback, oppure per creare un pacchetto di supporto, utile all'assistenza durante l'analisi degli errori.

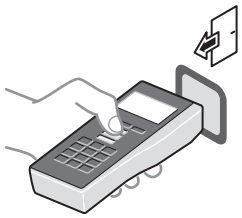
Sono disponibili i seguenti dati:

- Info (dati di stato)
- Traceback
- Configurazione
- Aggiornamento CardLink
- Diagnosi dati

I dati di configurazione dei componenti esistenti vengono sovrascritti dopo la conferma sul Programmer.

Il Traceback e la configurazione devono essere trasferiti con il programmer al software di sistema per la valutazione.

7.5.4.1 Importazione da cilindro digitale, c-lever e lettore



✓ Supporto master valido disponibile

1. Premere il tasto menu Importa.
   ⇨ Apertura del menu Importa.
2. Accedere al componente tramite master.

Attivare l'elettronica della serratura per armadietti 21 10 premendo brevemente la porta.

3. Menu, per esempio selezionare Configurazione.
4. Premere il tasto INVIO.

⇨ La configurazione del componente viene aggiornata e confermata.

7.6 Mobile Access

7.6.1 Requisiti di sistema

Firmware/Software di sistema

Funzione	Firmware	Software di sistema		
		Kaba exos 9300	**MATRIX**	**KEM**
Mobile Access	Si veda capitolo validità > Opzione Mobile Access	dalla versione 4.0.73	MATRIX Professional dalla versione 3.2.x, con opzione Mobile Access MATRIX ONE dalla versione 3.7	dalla versione 6.0

7.6.2 Inizializzazione del dispositivo per il Mobile Access

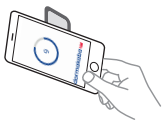
Requisiti preliminari

Generalità	• L'impianto di controllo degli accessi è configurato da dormakaba presso Legic Connect
Software del sistema	• La versione installata del software di sistema supporta Mobile Access. • Il collegamento con Legic Connect è realizzato. • Il dispositivo è configurato nel software di sistema per Mobile Access. • La configurazione è trasmessa sul Programmer.
Dispositivo	• Il dispositivo è installato e pronto per l'uso. • La tecnologia dei supporti è fissata, si veda il capitolo Tecnologia dei supporti. • La configurazione è trasferita dal Programmer al dispositivo.
Smartphone	• La VCP Installer è installata e registrata su Legic Connect con il numero di telefono. Inserire il codice di registrazione ricevuto per SMS. • L'accesso a internet è possibile (WLAN o dati mobili). • La password per il file VCP è nota.

Procedura

Trasferire la chiave Bluetooth/NFC sul dispositivo

- Tenere il mastermedium per ca. 1 s davanti all'antenna.
- Sullo Smartphone avviare il VCP Installer.
- Selezionare il file VCP.
  - Se non è disponibile il file VCP desiderato, selezionare "Aggiorna". Lo smartphone, successivamente, scarica il file VCP .
- Premere "Invia".
- Inserire la password per il file VCP.



- Tenere lo Smartphone davanti al dispositivo di lettura.

Segnalazione/indicazione		
	Dispositivo/antenna	**Smartphone**
Durante la trasmissione dei dati:	• luce verde accesa.	
Alla conclusione dell'inizializzazione:	• sono emessi 3 segnali acustici.	• Verde • Numero di serie del dispositivo
Il dispositivo è inizializzato.		
In caso di inizializzazione non conclusa correttamente:	• 1 bip breve. • Luce rossa brevemente accesa. • 1 bip lungo. • Luce rossa brevemente accesa.	• Rosso

Segnalazione/indicazione		
	Dispositivo/antenna	**Smartphone**
	• 1 bip breve.	

7.6.3 Inizializzazione del dispositivo per evolo smart

L'app evolo smart guida l'utente attraverso la procedura di inizializzazione del componente.

7.6.4 Regolazione della potenza del segnale Bluetooth

Modificare i valori predefiniti solo quando ciò è strettamente necessario.

- Dispositivi senza collegamento wireless:
  regolare la potenza del segnale Bluetooth nel sistema principale e trasferirla sul dispositivo con l'aiuto del Programmer.
- Dispositivi con collegamento wireless:
  regolare l'intensità del segnale Bluetooth nel sistema superiore e trasferirlo sul dispositivo tramite wireless gateway.

Si veda anche la linea guida di pianificazione Mobile Access.

7.7 Inizializzazione di componenti wireless

Per poter utilizzare i componenti in modalità wireless, deve essere effettuata una messa in funzione wireless.

Ulteriori informazioni sul wireless si trovano nella linea guida di pianificazione wireless e nel manuale tecnico del gateway 90 40-K7.

Requisiti preliminari

- Il gateway corrispondente è stato creato e configurato nel software di sistema.
- Il componente è stato creato nel software di sistema.
- Il componente è configurato per la modalità wireless.

Quando si utilizzano più gateway, avviare la messa in funzione wireless sempre su un solo gateway.
In caso contrario, i componenti potrebbero connettersi a un gateway non desiderato.

Avvio della messa in funzione wireless sul gateway:
Tramite interfaccia web

1. Nel file manager, selezionare il gateway per la messa in funzione.
2. Avviare l'interfaccia web del gateway.
3. Richiamare la funzione 'Messa in funzione wireless'.
4. Impostare l'intervallo di tempo per la messa in funzione.
   ⇨ In questo intervallo di tempo i componenti possono essere collegati al gateway.
5. Avviare la messa in funzione wireless.

Tramite software di sistema

✓ Il gateway per la messa in funzione è stato creato e configurato nel software di sistema.

1. Nel software di sistema, selezionare il gateway per la messa in funzione.
2. Richiamare la funzione 'Messa in funzione wireless'.
3. Impostare l'intervallo di tempo per la messa in funzione.
   ⇨ In questo intervallo di tempo i componenti possono essere collegati al gateway.
4. Avviare la messa in funzione wireless.

Se non è stato possibile mettere in funzione tutti i componenti necessari entro l'intervallo di tempo impostato, la procedura può essere ripetuta. I componenti già collegati al gateway rimangono collegati.

Collegare i componenti

✓ Il gateway è stato creato.

✓ La configurazione wireless del componente è stata trasmessa sul programmer oppure il componente è già configurato per il funzionamento wireless.

✓ La messa in funzione wireless sul gateway è stata attivata.

1. Registrarsi nel sistema del componente tramite supporto master.
2. Aprire il menu del Programmer 'Impostazioni attuatore'.
3. Scegliere il sottomenu Wireless.
4. Selezionare **Connetti**.
5. Confermare con INVIO.
   ⇨ Ricerca della rete... (viene ricercata la rete.)
   ⇨ Gateway (GW) trovato.
   ⇨ Collegamento al GW eseguito.
   ⇨ Messa in funzione...
   ⇨ • Connesso al GW.

⇨ La messa in funzione wireless del dispositivo è stata completata.

7.8 Impostare proprietà e funzioni di un componente

Con il programmer è possibile modificare le seguenti proprietà di un componente:

- La data e l'ora dell'orologio.
- La segnalazione acustica e ottica.
- L'orario di apertura (valore di default: 6 s).
- La versione firmware.
- Il reset INI.
- Connettere un componente wireless con un wireless gateway.

Funzioni principali
Le due funzioni principali, eseguibili con il programmer sui componenti, sono l'**esportazione** e l'**importazione** di dati. Entrambe le funzioni vengono eseguite con il programmer con l'interfaccia radio (NFC) o con il cavo di programmazione.

7.9 Reset (reset INI)

Il reset INI permette di riportare i componenti allo stato di consegna.

AVVISO

Perdita di dati

In un reset INI, tutte le impostazioni e i dati memorizzati in precedenza vengono cancellati sul modulo elettronico.

Nei componenti wireless viene interrotta la connessione con il gateway.

È possibile eseguire questa operazione nei seguenti modi:

Reset con supporti master
Il reset INI viene eseguito se il supporto master corrispondente dei componenti viene tenuto davanti all'antenna.

Reset con Programmer 1460
Il reset INI può essere eseguito anche tramite il programmer. Per questa variante sarà necessario disporre anche del supporto master corrispondente.

Reset INI con pinzetta e supporti master validi
Alcuni componenti dispongono di contatti di reset INI sul modulo elettronico. Per effettuare il reset INI, cortocircuitare questi contatti con una pinzetta a conduzione elettrica.

Con interruttore DIP
Alcuni componenti dispongono di interruttore DIP. Azionare l'interruttore DIP specifico per eseguire il reset INI.

Ulteriori informazioni relative al reset INI sono fornite nella documentazione sul componente.

7.9.1 Panoramica delle varianti di reset INI dei componenti

Nella tabella seguente vengono riportate le varianti di reset INI e le differenze per E300 (V4) e V3.

Alcuni componenti dispongono di contatti di reset INI. Cortocircuitare questi contatti per circa 3 secondi con una pinzetta a conduzione elettrica per eseguire il reset INI.

Componente	Master Admin	Programmer 1460[1]	Pinzetta	Interruttore DIP
c-lever	✓	✓	✓	—
c-lever pro	✓	✓	✓	—
c-lever pro TouchGo	✓	—	✓	—
c-lever compact	✓	✓	—	—
Cilindro digitale	✓	✓	✓ [2]	—
Cilindro meccatronico Risvolto	✓	✓	—[4]	—
Cilindro meccatronico Applicazione/ Compatto	✓	✓	✓ [2]	—
Lettore remoto	✓	✓	—	✓ [3]
Lettore compatto	✓	✓	—	✓ [3]
Serratura per armadietti 21 10	✓	✓ [2]	✓	—

Legenda:

1 Presentare il supporto master.
2 Presentare il supporto master oppure un supporto utente autorizzato.
3 Impostare l'interruttore DIP 6 su ON.
4 Punti di reset nel modulo con risvolto

Le informazioni relative al reset di altri componenti sono fornite nei rispettivi manuali.

Eseguire il reset INI sempre secondo quanto indicato nel manuale del dispositivo.

7.10 Risparmio energetico

Componenti standalone
La quantità di energia della batteria e il consumo di energia determinano per quanto tempo sono in grado di funzionare i componenti standalone prima che la riserva di energia si sia esaurita. Attraverso varie impostazioni è possibile risparmiare energia.

7.10.1 Disattivare funzioni

Disattivare funzioni non necessarie per risparmiare energia

A seconda del tipo di dispositivo e dell'impiego, possono essere disattivate una o più funzioni se non sono richieste per le finalità d'uso. Ciò contribuisce a risparmiare energia e a prolungare l'intervallo tra le sostituzioni della batteria.

Esempi di funzioni che si possono disattivare:

- segnalazione acustica (buzzer)
- segnalazione ottica (anello luminoso)
- traceback del supporto
- Tecnologie non richieste
- Funzione wireless (se non richiesta)
- Se possibile, ridurre la potenza di trasmissione wireless.
- Mobile Access (se non richiesto)

7.10.2 Funzione Object in Field

Il componente verifica periodicamente se un supporto si trova nel campo dell'antenna. Per risparmiare energia, l'intervallo di tempo tra due verifiche viene prolungato. In caso di "Object in Field" dinamica, questo periodo resoconto viene progressivamente ampliato fino al valore massimo. Se un supporto viene esposto, la procedura inizia nuovamente. In caso di esposizione di un supporto è possibile un tempo di reazione più lungo.

La funzione "Object in Field" (OIF) viene parametrizzata nel software di sistema.

Tabella: Risparmio energetico grazie all'OIF dinamico. I valori sono approssimativi. I risparmi energetici effettivi dipendono anche da altri fattori e impostazioni.

Caso pratico	**Impostazioni**		**Rispar-mio**	**Effetti**
Esempi:	**OiF Intervallo**	**OIF OiF**	**massimo**	
Impostazione standard dei componenti. **Accessi molto frequentati**	300 ms	OFF	0%	Normale
Accessi poco frequentati	300 ms	ON 30 min	15%	Tempo di reazione prolungato per il primo supporto esposto dopo una lunga pausa. Normale in altri supporti nell'arco di tempo impostato.
• 20 procedure di mattina e di sera entro il periodo impostato Nel frattempo, in 10 ore, 1 procedura ogni ora.	300 ms	ON 30 min	19%	
• In 10 ore, 1 procedura ogni ora.	300 ms	ON 30 min	22%	
Accessi raramente necessari • 2 procedure di mattina e 2 di sera entro il periodo impostato. Nel frattempo nessuna procedura.	300 ms	ON 30 min	30%	Periodo di reazione prolungato durante il primo utilizzo dopo una pausa prolungata. • La lettura di un supporto esposto può durare fino a 1 s.
• Lunghi periodi di riposo tra i procedimenti • Una o più giornate senza procedimenti	1000 ms	OFF	34%	

8 Segnali

Questo capitolo descrive i due tipi di segnale, il loro significato e rispettive segnalazioni.

I segnali acustici e gli indicatori visivi vengono emessi quando i supporti vengono rilevati dall'antenna del componente.
I segnali e i display per l'autorizzazione all'accesso possono essere attivati o disattivati individualmente tramite la catena degli strumenti.

Simboli

Simboli		Descrizione
		Segnale acustico
		Segnale ottico

8.1 Durata del segnale

Quando vengono presentati supporti utente con autorizzazione di accesso, vengono emessi i seguenti segnali acustici (bip) e visivi (LED).

Segnali / Display	Duration	Duration
Bip / LED acceso	molto breve	40 ms
Bip / LED acceso	Breve	120 ms
Bip / LED acceso	Lungo	600 ms
Bip / LED acceso	molto lungo	3000 ms

8.2 Autorizzazioni d'accesso

Componenti e supporti sono inizializzati e programmati.

Segnalazioni di funzionamento:

Significato	[1]	[1]	Supporti
Autorizzato (Apri)	1x breve	1x breve verde	Utente: supporti
Non autorizzato (Non aprire)	4x brevi	4x brevi rossi	Utente: supporti
Autorizzato (Chiudi) [3]	1x breve	1x breve verde 1x lungo rosso	Utente: supporti
Autorizzato (Chiudi) [2, 3]	1x breve 1x lungo	—	Utente: supporti

Legenda:

[1] Segnali acustici e visualizzazioni si possono attivare o disattivare con la catena di strumenti (con il software di sistema , ad es. KEM ,e il programmer).

[2] Componenti senza visualizzazione.

[3] Chiusura con supporti autorizzati o premendo il tasto (c-lever), come per esempio nelle modalità Office, Escape Return e Pass.

8.3 Autorizzazioni Pass-Lock (c-lever)

Significato			Supporti
Attivare	1x lungo	—	Utente: supporti

Significato			Supporti
Disattivare (chiudere)	1x breve	—	Utente: supporti
Stato (Aperto)	—	ogni 3 s arancione molto breve	Utente: supporti

8.4 Autorizzazioni Modalità Escape-Return e Pass (c-lever)

Significato			Attività
Attivare	1x lungo	1x arancione molto lungo (3 s)	Premere il tasto per 2 secondi
Disattivare (chiudere)	1x lungo	5x arancione molto corto	Premere il tasto per 2 secondi
Autorizzato (chiudere)	1x breve	1x verde corto 1x lungo rosso	Utente: supporti
Stato (Aperto)	—	1x arancione molto lungo (3 s)	Premere brevemente il tasto
Stato (non aperto)	—	5x arancione molto corto	Premere brevemente il tasto

8.5 Segnalazioni di applicazione della tessera di sicurezza C2

Se si applica la tessera di sicurezza C2, sono emessi i seguenti segnali acustici e visualizzazioni ottiche.

Nota: L'autorizzazione alla scrittura viene cancellata con il reset INI.

Applicazione della tessera di sicurezza C2:

Procedura			Supporti
Primo passo: inizializzare i componenti	1x breve	verde, finché il supporto master si trova nel campo dell'unità di rilevamento	Master A oppure master B
Programmare l'autorizzazione alla scrittura.	—	verde, finché la procedura non viene terminata	Tenere la tessera di sicurezza C2 nel campo dell'antenna per 15 s.
Fine: eliminazione in corso della programmazione dell'autorizzazione alla scrittura.	3x brevi	—	—
Cancellare l'autorizzazione di scrittura con la tessera di sicurezza C2	3x brevi	—	—

8.6 Segnalazioni di programmazione

Segnalazioni durante la programmazione:

Procedura			Supporti
Primo passo: Supporti da programmare	1x breve	Il LED si illumina quando i supporti si trovano nel campo dell'unità di rilevamento. Non si illumina quando viene emesso un segnale acustico.	Master A e Master B
Conferma di programmazione dei supporti [2]	1x breve		Master A e Master B
Supporto cancellato [2]	dopo 3 s 2x brevi		Utente: supporti
Tutti i supporti cancellati [2]	dopo 10 s [3] 2x brevi		Master B (in struttura A/B)
	dopo 10 s [4] 1x lungo 1x breve		
Fine: Supporti da programmare	1x lungo		Master A e Master B
Errore durante la programmazione	1x lungo	1x breve rosso	
Errore durante la programmazione [1]	2x lunghi	—	

Legenda:

[1] Componenti senza visualizzazione

[2] Solo per funzionamento whitelist senza sistema host

[3] Prima della versione 42 del firmware

[4] Dalla versione 42 del firmware

8.7 Wireless

Significato			Strumento
Identificare componente [6]	1x breve	1x lungo verde 1x breve verde	

Legenda:

[6] Ogni 3 s i segnali si ripetono fino alla conclusione della procedura.

8.8 Segnalazioni di reset

Nota: L'autorizzazione alla scrittura viene cancellata con il reset INI.

Significato			Strumento
Conferma il reset	dopo 3 s 2x brevi	—	Pinzetta Mettere in cortocircuito i contatti del reset INI
Conferma il reset (whitelist)	dopo 10 s 1x lungo 1x breve dopo 15 s 2x brevi		Supporti master
Conferma il reset (CardLink)	dopo 15 s 2x brevi		Supporti master
Conferma il reset	2x brevi		Programmer 1460

8.9 Messaggi di errore e di guasto

Significato			Supporti
Batteria “scarica” FW 42.XX	1x molto breve	9x molto breve rosso[3]	Supporti utente Master A e Master B
Batteria “scarica” FW 42.XX[1]	9x molto brevi[3]	—	Supporti utente Master A e Master B
Batteria “Scarica”	1x molto lungo[3]	—	Supporti utente Master A e Master B
Impossibile completare l'autotest.[5]	8x brevi	8x brevi rossi	Supporti utente
Supporti non autorizzati[4]	4x brevi	4x brevi rossi	Supporti utente
Guasto dell'orologio interno al componente[2]	1x lungo 1x breve 1x lungo	1x breve verde	Supporti utente Master A e Master B
Impossibile creare tutte le sitekey	1x breve 1x lungo 1x breve	2x breve rosso	Master A e Master B (MIFARE)
Impossibile creare tutte le chiavi dell'impianto			Supporti di servizio

Legenda:

1 Componenti senza visualizzazione.

2 A condizione che l'orologio sia stato correttamente impostato in precedenza.

3 Successivamente 1x breve verde seguito dall'apertura del componente.

4 La batteria "Quasi scarica" non viene segnalata.

5 Funzione solo per c-lever, cilindri meccatronici e cilindri digitali.
Nota: Si consiglia di controllare lo stato sui componenti corrispondenti.

9 Manutenzione del sistema

9.1 Piano di manutenzione



AVVISO

Rischi per i componenti elettronici causati da scariche elettrostatiche.

La manipolazione impropria di schede o componenti elettronici può causare danni che portano a guasti totali o a errori saltuari.

- Durante l'installazione e la riparazione del prodotto è necessario osservare le misure generali di protezione ESD.

Eseguire le seguenti attività per consentire il funzionamento di impianti di chiusura e componenti per lungo tempo senza guasti.

I dettagli sugli interventi di manutenzione sono riportati nelle istruzioni per l'uso separate dei componenti corrispondenti.



I periodi di manutenzione e l'aspettativa di vita indicati per parti e componenti possono variare a seconda delle sollecitazioni e condizioni ambientali.
I valori indicati si riferiscono a un livello medio di sollecitazioni.

Verifica

- Eseguire un controllo del funzionamento del componente ogni 12 mesi come da istruzioni.
- Verificare ed impostare l'ora ogni 12 mesi con il Programmer 1460.
  In caso di funzionamento tramite wireless la sincronizzazione dell'orologio avviene tramite il wireless gateway.

Aggiornamento
Per un adeguamento delle funzioni, eseguire un aggiornamento firmware annuale o secondo necessità. Evitare di differenziare gli stati firmware dei componenti di un impianto.

Sostituire le batterie
Nelle seguenti tabelle sono riportati gli intervalli medi in base a cui sostituire le batterie dei componenti. La durata media dipende dal tipo di batteria, dalle condizioni ambientali, nonché dalla configurazione utilizzata (Whitelist/CardLink), dalla dotazione (standalone/wireless) e dalle opzioni impostate (per esempio la segnalazione acustica).

Controllare lo stato delle batterie ogni 12 mesi. All'occorrenza sostituire le batterie.

- Condizioni ambientali: Vedi specifiche del produttore della batteria.
- Tipo di batteria: litio. Utilizzare solo i tipi di batterie consigliati.

9.2 Durata delle batterie

La durata della batteria come fonte di energia per componenti standalone dipende da numerosi fattori.

- Oscillazioni della qualità del produttore delle batterie.
- Tipo delle funzioni di un componente utilizzate.
- Numero delle funzioni di un componente utilizzate e/o combinate.
- Numero delle procedure in un determinato periodo, ad es. ogni giorno/settimana/mese/anno.
- Condizioni ambientali come temperatura, umidità dell'aria ecc.

Il componente segnala il livello basso della batteria tramite segnali.

Esempi di durata della batteria nei vari componenti:

Condizioni presupposte dalla tabella:

- Temperatura media 20 °C

- Funzionamento standalone
- Modalità di accesso Whitelist
- Senza segnalazione acustica

Componente	Attivazioni per giorno lavorativo	Intervallo
c-lever pro	ca. 250	24 mesi
c-lever		
c-lever compact	ca. 100	24 mesi
Cilindro digitale	ca. 100	12 mesi
	max. 50	24 mesi
Cilindro meccatronico variante con risvolto	ca. 400	12 mesi
	ca. 100	24 mesi
Cilindro meccatronico varianti - Compatto - Applicazione	ca. 50	24 mesi
Serratura per armadietti 21 10	ca. 100	24 mesi

Batterie nei supporti TouchGo:

Componenti	modello di batteria	Tensione	Art.	Campo di temperatura	Durata
Portachiavi	CR2450	3 V	litio	da –20 fino a 65 °C	ca. 1 anno
Braccialetto	CR2450	3 V	litio	da –20 fino a 65 °C	ca. 1 anno
Porta-schede	CR2430	3 V	litio	da –20 fino a 65 °C	ca. 1 anno

9.3 Tempo tampone nella sostituzione della batteria

Per la sostituzione della batteria occorre tenere presente che è disponibile solo un breve intervallo di tempo prima che le impostazioni dell'orologio dei componenti vadano perse (vedere la tabella seguente).

Nota: controllare le impostazioni dell'orologio nei componenti dopo la sostituzione della batteria.

Tempi tampone:

Componenti	Tempo tampone
c-lever	< 60 s
c-lever pro	< 45 s
c-lever compact	< 45 s
Cilindro digitale	< 45 s
Cilindro meccatronico • Risvolto • Compatto • Applicazione	< 45 s
Serratura per armadietti 21 10	< 120 s

9.4 Apertura a batterie scariche

Se sono state ignorate tutte le segnalazioni di allarme fino al completo esaurimento delle batterie, i componenti possono essere aperti solo con il dispositivo di alimentazione di emergenza del Programmer 1460.

Per una descrizione dell'alimentazione di emergenza (apertura di emergenza), consultare le istruzioni per l'uso del Programmer 1460.

Nel cilindro digitale e nel c-lever compact la/le batteria/e si trovano all'esterno. Dopo la sostituzione, controllare l'orologio del componente con il Programmer 1460 o tramite wireless e, all'occorrenza, regolarlo.

La serratura per armadietti 21 10 non dispone di una funzione di apertura di emergenza in caso di batteria scarica. Quando la batteria è scarica, la serratura deve essere forzata.

- Sostituire la batteria quando si visualizza “Batteria scarica”

9.4.1 Supporto temporaneo di apertura di emergenza

Un supporto di apertura di emergenza è possibile dalla versione FW 42.36.

Se la batteria è scarica e si è persa la configurazione, è ancora possibile programmare manualmente un supporto temporaneo di apertura di emergenza. In questo modo la porta può essere aperta una volta per sostituire la batteria. L'applicazione del supporto di apertura di emergenza è possibile per

- c-lever
- c-lever pro
- Cilindro MC

Il supporto di apertura di emergenza viene programmato mediante il supporto master nella memoria RAM del componente ed è valido solo 1 minuto o fino al prossimo riavvio.

Sulla segnalazione si veda il capitolo Segnalazioni di programmazione [▶ 8.6].

Requisiti preliminari

- Batteria completamente scarica o batteria scarica con alimentazione di emergenza
- È presente il supporto master.
- Il supporto di apertura di emergenza è un supporto utente specifico per l'impianto.
- Funzionamento porta: Whitelist
- La whitelist è vuota.

Procedura

1. Presentare il supporto master.
   ⇨ Segnalazione in caso di batteria scarica: Batteria scarica, seguita da inizio della modalità di programmazione
   ⇨ Segnalazione in presenza di alimentazione di emergenza: Inizio programmazione
2. Presentare il supporto utente previsto come supporto di apertura di emergenza.
   ⇨ È possibile solo 1 supporto di apertura di emergenza
   ⇨ Il salvataggio viene segnalato.
3. Presentare il supporto master.

⇨ Al termine della procedura di programmazione, c'è 1 minuto di tempo per aprire la porta con il supporto di apertura di emergenza. Dopo, il supporto viene nuovamente cancellato dalla memoria.

9.5 Configurazioni e Traceback

La correttezza dei valori impostati per data e ora assicurano un'aggiornata gestione del tempo con i componenti.

I componenti che sono connessi tramite la funzione wireless al software del sistema sono aggiornati tramite il gateway (ad es. ora, configurazioni). Il traceback può essere letto con software di sistema.

Con gestione meramente standalone sono trasmesse le configurazioni con il programmer o possono essere modificate con esso (ad es. impostazione dell'ora).
Con un programmer può essere letto il traceback ed essere trasferito al software di sistema per la valutazione al software del sistema.

Ulteriori passaggi sono descritti nelle istruzioni per l'uso del Programmer 1460.

9.6 Aggiornamento firmware dei componenti

Il firmware dei componenti può essere aggiornato nel sottosistema evolo.

Le nuove versioni del firmware sono trasmesse con il programmer o tramite wireless ai componenti standalone.

Nota: i componenti Multi RFID (MRD) con programmazione manuale devono essere controllati dopo un aggiornamento firmware sulla programmazione manuale con i supporti corrispondenti. All'occorrenza, è necessario eseguire un reset INI.

In alcuni componenti (lettore con funzionamento online) determinate funzioni possono essere modificate aggiornando il firmware.

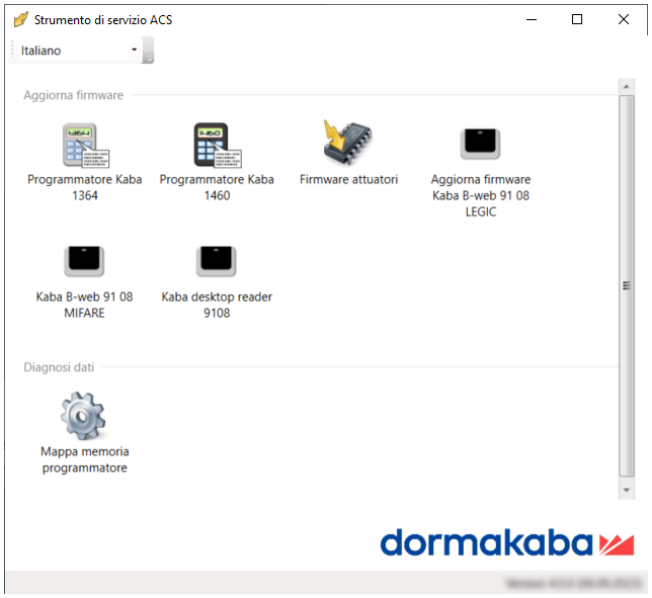
Se le autorizzazioni di lettura/scrittura sono disponibili sul componente, dal firmware 42.40 del componente e dal firmware 01.36 del Programmer vale quanto segue:
Le autorizzazioni di lettura/scrittura (dati 'd'iniziazione') **non** vengono cancellate con l'aggiornamento del firmware.
Se si desidera cancellare le autorizzazioni di lettura/scrittura, è necessario eseguire un reset INI.

Una descrizione dettagliata è contenuta nelle istruzioni per l'uso del Programmer 1460.

9.7 dormakaba ACS Service Tool

Il dormakaba ACS Service Tool è un programma ausiliario per l'aggiornamento dei dati firmware e la creazione di diagnosi.

Lo strumento può essere avviato anche direttamente, ovvero senza che il software di sistema sia in esecuzione. Per avviarlo, selezionare *Menu Start -> Programmi -> Kaba -> dormakaba ACS Service Tool*.



Programmer 1364	Procedura guidata per l'aggiornamento del firmware del Programmer.
Programmer 1460	Procedura guidata per l'aggiornamento del firmware del Programmer.
Firmware attuatori	Procedura guidata per il trasferimento del firmware dei componenti al Programmer.

Lettore da tavolo 91 08 LEGIC/MIFARE/MRD	Procedura guidata per l'aggiornamento del firmware del lettore da tavolo per la tecnologia selezionata.
Immagine di memoria Programmer 1460	Procedura guidata per la creazione di un file ZIP con il contenuto della memoria del Programmer. Uno strumento per la soluzione dei problemi nei casi di assistenza.

Prima dell'aggiornamento, il firmware deve essere scaricato da Internet/Extranet su un disco fisso locale.

Il Programmer 1364 non è più disponibile né supportato. Ultimo firmware scaricabile: 1.38

Note

www.dormakaba.com

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

www.dormakaba.com