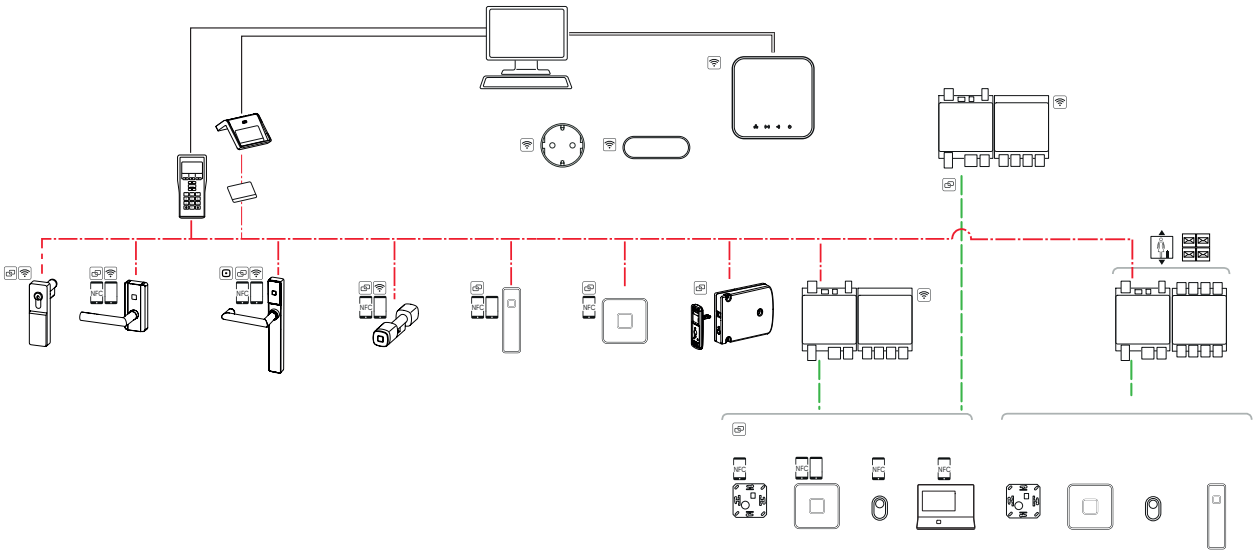
Description du système evolo

Description du système



Public - 11/2026

FR

Table des matières

1 À propos de ce document 5
1.1 Nouvelles fonctions et mises à jour 5
1.2 Validité 5
1.3 Groupe cible 5
1.4 Contenu et objectif 6
1.5 Disponibilité des documents 6
1.6 Documents complémentaires 6
1.7 Abréviations/Définition de termes 6
1.8 Mises en garde 8

2 Vue d'ensemble 9
2.1 Autorisation 9
2.2 Composants 9
2.3 Logiciel système 11
2.3.1 Topologies 11
2.3.2 Chaîne d'outils 12
2.4 Options d'accès par smartphone 13
2.4.1 Applications Mobile Access 13
2.4.2 Accès par Wallet (Apple Wallet et Google Wallet) 14
2.5 Médias 14
2.5.1 Médias master 16
2.5.2 Médias utilisateurs 17
2.6 Structures de programmation 18
2.6.1 Structure A/B et B 18
2.7 Prise en charge d'OSS-SO 20

3 Types d'autorisations et fonctions 21
3.1 Numéro d'identification 21
3.2 Niveau de système 21
3.3 Autorisation Whitelist 22
3.3.1 Autorisation Whitelist avec profil de temps 23
3.4 Autorisation CardLink 25
3.4.1 Droits d'accès 25
3.4.2 Validation 27
3.4.3 Valider les médias 27
3.4.4 Médias perdus 28
3.4.5 Liste noire 29
3.4.6 Médias de service 29
3.4.7 Information sur l'état 29
3.4.8 Traceback des médias 29
3.5 Access on Card 30
3.6 Mode mixte 30
3.7 Médias non autorisés 30
3.8 Fonctions TimePro 30
3.8.1 Profil de temps Office 30
3.8.2 Profil de temps Day/Night 32
3.9 Fonctions avancées 32
3.9.1 Composants wireless 32
3.9.2 Traceback de composants 35
3.9.3 S-Module 35
3.9.4 Fonction Retour (Escape Return) avec la c-lever pro 35
3.9.5 Mode Pass avec c-lever pro 35
3.9.6 Pass-Lock avec c-lever pro 36
3.9.7 Médias d'intervention 36
3.9.8 Désactiver la programmation manuelle 37
3.10 TouchGo 37
3.10.1 Fonctionnement RCID 37
3.10.2 Aspects de sécurité 37
3.10.3 TouchGo E110 38
3.10.4 TouchGo E310 38

3.11 Sélection de vestiaire libre avec les serrures d'armoire 21 10 et 21 20 39
3.12 Boîte aux lettres/ascenseur 39

4 Variantes de système 40
4.1 Programmation Whitelist 40
4.1.1 Autorisation Whitelist sans chaîne d'outils 40
4.1.2 Autorisation Whitelist avec chaîne d'outils 41
4.2 Programmation CardLink 42
4.2.1 Autorisation CardLink via lecteur de table 42
4.2.2 Autorisation CardLink via lecteur de mise à jour 43
4.2.3 Autorisation CardLink via terminal 44
4.3 Vue d'ensemble des variantes de micrologiciels 45

5 Fonctions de sécurité 47
5.1 Les degrés de sécurité LEGIC 47
5.2 Sécurité avec autorisations CardLink LEGIC 47
5.3 Sécurité avec l'autorisation Whitelist LEGIC 48
5.4 Les degrés de sécurité MIFARE 48
5.5 Sécurité avec autorisations CardLink MIFARE 49
5.6 Sécurité avec l'autorisation Whitelist MIFARE 49
5.7 Master T 50

6 Composants 51
6.1 Espaces de mémoire 51
6.2 Données techniques 51
6.3 Médias master 54
6.4 Cartes de sécurité 54
6.5 Chaîne d'outils 55

7 Programmer / configurer les composants 57
7.1 Définir la technologie de média 57
7.2 Méthodes de programmation et configuration 57
7.3 Programmer des produits TouchGo 57
7.3.1 Programmer TouchGo E310 58
7.3.2 Médias utilisateurs perdus/défectueux 65
7.4 Programmer avec des médias 65
7.4.1 Cartes 66
7.4.2 Clé 72
7.4.3 Réinitialisation INI avec des médias master 77
7.5 Programmation avec logiciel système 79
7.5.1 Logiciel système pour les composants evolo 80
7.5.2 Programmation avec logiciel système et programmeur 80
7.5.3 Exportation vers des composants 80
7.5.4 Importation à partir des composants 81
7.6 Mobile Access 81
7.6.1 Configuration requise du système 81
7.6.2 Initialisation de l'appareil pour Mobile Access 82
7.6.3 Initialisation de l'appareil pour evolo smart 83
7.6.4 Régler la puissance du signal Bluetooth 83
7.7 Initialisation des composants wireless 83
7.8 Réglage des propriétés et des fonctions d'un composant 84
7.9 Réinitialisation (INI-Reset) 84
7.9.1 Vue d'ensemble des variantes INI-Reset des composants 85
7.10 Économiser de l'énergie 86
7.10.1 Désactiver les fonctions 86
7.10.2 Fonction Object in Field 87

8 Signaux 88
8.1 Durée du signal 88
8.2 Autorisations d'accès 88
8.3 Autorisations Pass-Lock (c-lever) 88
8.4 Autorisations Escape Return et Mode Pass (c-lever) 89
8.5 Messages lors de l'utilisation de la carte de sécurité C2 89

8.6 Messages de programmation 89
8.7 Composants 90
8.8 Messages de réinitialisation 91
8.9 Messages d'erreur et de dysfonctionnement 92

9 Maintenance du système 93
9.1 Plan de maintenance 93
9.2 Durée de vie des piles 93
9.3 Période tampon pour le remplacement des piles 94
9.4 Ouverture en cas de piles déchargées 94
9.4.1 Média d'ouverture d'urgence temporaire 95
9.5 Configurations et Traceback 95
9.6 Mise à jour FW des composants 96
9.7 dormakaba ACS Service Tool 96

1 À propos de ce document

1.1 Nouvelles fonctions et mises à jour

Le tableau suivant contient les améliorations apportées à cette version du sous-système, de ses composants associés ou du logiciel/micrologiciel.

Modification	Description	Introduit dans
Délai d'activation Pass-Lock	Afin d'éviter une activation involontaire de Pass-Lock, un délai configurable peut être défini. Il faut maintenir la touche enfoncée pendant toute la durée configurée avant que Pass-Lock ne soit activé. Voir le chapitre Pass-Lock avec c-lever pro [▶ 3.9.6].	42.48
Médias d'intervention	Un groupe dédié de médias d'intervention peut être défini pour maintenir l'accès lorsque Pass-Lock est actif ou lorsqu'un système de détection d'intrusion (IDS) est armé. Voir Médias d'intervention [▶ 3.9.7].	42.48
Prise en charge de Google Wallet	Google Wallet peut être utilisé comme média utilisateur via NFC sur les composants evolo pris en charge. Voir le chapitre Accès par Wallet (Apple Wallet et Google Wallet) [▶ 2.4.2].	42.48
Prise en charge d'Apple Wallet	Apple Wallet peut être utilisé comme média utilisateur via NFC sur les composants evolo pris en charge. Voir le chapitre Accès par Wallet (Apple Wallet et Google Wallet) [▶ 2.4.2].	42.46
Option Access on Card (AoC) pour une validité illimitée	Lorsque vous utilisez MATRIX, vous pouvez définir une validité d'accès illimitée pour un utilisateur si les exigences commerciales du client l'exigent. Voir le chapitre Access on Card [▶ 3.5].	42.40
Mise à jour de la désignation du hub de communication	Pour tenir compte des dernières améliorations, ce manuel décrit le hub de communication dans sa version actuelle **90 40-K7**.	-
c-lever air discontinuée	Le produit n'est plus proposé aux clients et n'est plus mentionné dans ce manuel.	-

1.2 Validité

Ce document décrit le sous-système evolo pour les technologies RFID LEGIC, MIFARE et MRD (Multi RFID Device). La technologie MRD est utilisée sur les nouvelles installations.

Ce document décrit le sous-système evolo pour l'utilisation des technologies mobiles Bluetooth® et NFC.

La description inclut les composants autonomes, wireless, Bluetooth® et NFC.

Version du micrologiciel installée sur les composants : version 42.38 ou supérieure

Les descriptions et exemples de ce manuel portant sur l'utilisation des composants avec des systèmes hôtes se réfèrent à l'utilisation avec KEM. L'intégration du sous-système evolo dans les systèmes hôtes est décrite dans la documentation des systèmes hôtes correspondants.

1.3 Groupe cible

Cette documentation est exclusivement destinée aux techniciens.

Les descriptions présupposent que ces techniciens ont été formés par le fabricant. Les descriptions ne remplacent aucune formation sur les produits.

Pour des raisons de sécurité du périphérique, les opérations d'installation, de maintenance et de réparation décrites dans cette documentation ne doivent être effectuées que par des techniciens, conformément à la norme EN 62368-1 (Équipements des technologies de l'audio/vidéo, de l'information et de la communication - Partie 1 : exigences de sécurité).

Le spécialiste est le nom des personnes titulaires d'une formation technique appropriée et ayant l'expérience de la technique de l'établissement. Les spécialistes s'attendent à utiliser leur formation et leur expérience pour détecter et réduire au minimum les risques liés à l'exécution des actes eux-mêmes et aux autres. Il est de la responsabilité du spécialiste que les conditions énoncées par le fabricant, ainsi que les prescriptions et normes applicables pour l'exécution de ces actes soient respectées.

Cette documentation sert également à l'information des personnes exerçant les fonctions suivantes :

- Planification et réalisation de projets
- Mise en service du produit au sein du réseau
- Connexion du produit au logiciel utilisateur par programmation d'applications client
- Personnalisation propre au client par paramétrage du produit

1.4 Contenu et objectif

Ce document contient les bases du système evolo et en donne une vue d'ensemble globale.

1.5 Disponibilité des documents

Des documentations supplémentaires sont disponible sur le lien suivant :

https://techdoc.dormakaba.com/cds

1.6 Documents complémentaires

Les documents suivants sont disponibles via le partenaire commercial:

- Documentation technique des composants utilisés
- Manuel du Programmer 1460
- Documentation du logiciel système utilisé
- Catalogue de produits dormakaba evolo

Option TouchGo

- Manuel d'utilisation de dormakaba c-lever pro TouchGo
- Directive de planification dormakaba c-lever pro TouchGo avec S-Module

Option wireless

- Directive de planification wireless

Option Mobile Access

- Directive de planification Mobile Access

1.7 Abréviations/Définition de termes

Pour une meilleure lisibilité, les désignations officielles de produits suivantes sont remplacées par des désignations abrégées.

Désignation de produit/Définition	Désignation abrégée
dormakaba evolo	evolo
Gestionnaire de porte dormakaba	Lecteur
Lecteur compact dormakaba	

Désignation de produit/Définition	Désignation abrégée
Cylindre digital dormakaba	Cylindre digital
Cylindre mécatronique en applique dormakaba	Cylindre mécatronique
Cylindre mécatronique compact dormakaba	
Cylindre mécatronique à têtière dormakaba	
Terminal dormakaba 94 20	Terminal
dormakaba c-lever pro TouchGo	TouchGo
dormakaba c-lever pro	c-lever
dormakaba c-lever compact	
Kaba c-lever	
Serrure d'armoire dormakaba 21 10	Serrure d'armoire
Wireless Gateway 90 40-K7	Hub de communication
Wireless Extender 90 41	Extender
Gestionnaire de porte dormakaba 91 15 (E320) avec module d'extension wireless 90 43	Wireless Reader
Lecteur de table dormakaba 91 08	Lecteur de table
Programmer dormakaba 1364	Programmer 1364
Programmer dormakaba 1460	Programmer 1460
dormakaba evolo Manager	KEM
Kaba exos 9300	exos
dormakaba MATRIX ONE	MATRIX
dormakaba MATRIX PRO	
dormakaba b-com	b-com
Numéro unique	UID
Numéro d'identification de la carte	CID
Identification par radiofréquence	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

Les symboles suivants représentent des signaux acoustiques ou visuels :

Symboles		Type de signal
		Signal acoustique
		Signal visuel

Les composants sans possibilité d'affichage visuel n'émettent pas de signal visuel.

1.8 Mises en garde

Le présent manuel contient des indications que vous devez respecter pour votre propre sécurité et pour prévenir tout dommage matériel. Les informations relatives à votre sécurité personnelle sont mises en évidence par un triangle de signalisation ; les indications relatives aux seuls dommages matériels ne possèdent pas de triangle de signalisation. Selon le niveau de danger, les mises en garde sont représentées comme suit dans un ordre décroissant :

⚠ DANGER

Risque élevé

Indique un danger imminent pouvant entraîner des blessures physiques graves, voire la mort.

⚠ AVERTISSEMENT

Risque moyen

Indique une situation potentiellement dangereuse pouvant entraîner des blessures physiques graves, voire la mort.

⚠ ATTENTION

Risque faible

Indique une situation potentiellement dangereuse pouvant entraîner des blessures physiques légères.

AVIS

Informations importantes concernant l'utilisation correcte du produit

Le non-respect de ces instructions peut entraîner des dysfonctionnements. Le produit peut être endommagé.

En présence de plusieurs niveaux de danger, la mise en garde du niveau le plus élevé est toujours utilisée. Lorsqu'une mise en garde concerne des dommages corporels, la même mise en garde peut en outre concerner des dommages matériels.

Autres symboles d'avertissement :


Danger en général


Risque d'explosion


Danger émanant d'une tension électrique


ESD : Danger émanant de décharges électrostatiques

Les conseils et informations utiles pour le fonctionnement en toute sécurité du produit sont signalés comme suit :

Conseils d'utilisation et informations utiles.
Ils permettent d'utiliser de manière optimale le produit et ses fonctions.

2 Vue d'ensemble

Le sous-système evolo est une combinaison de composants autonomes dont la configuration est transférée au moyen de la chaîne d'outils.

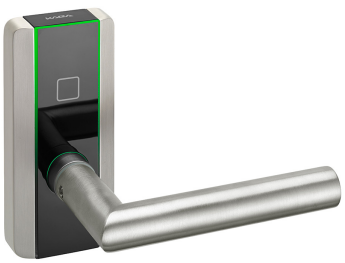
2.1 Autorisation

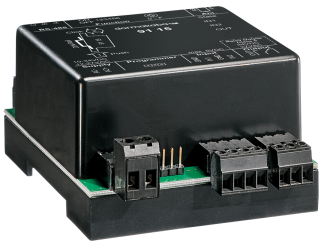
Description

Autorisation	Description
Whitelist	Les informations d'autorisation se trouvent dans les composants.
CardLink	Les informations d'autorisation se trouvent dans les médias utilisateurs.
Access on Card AoC	Utilisé uniquement sous MATRIX : Les informations d'autorisation se trouvent dans les médias utilisateurs. Vous trouverez plus d'informations sur AoC dans la documentation MATRIX.
OSS-SO	Norme ouverte. Pour obtenir de plus amples informations : http://www.oss-association.com/standards/oss-standard-offline/
Mobile Access	Avec Mobile Access, le smartphone devient un média utilisateur.

2.2 Composants

Composants électroniques dotés de diverses fonctions, pouvant être installés dans ou sur des portes.

	Aperçu du système Composants	
Numéro de produit	**Composant**	**Description**
		c-lever pro **Options :** • Wireless • Mobile Access • OSS-SO • TouchGo E110 uniquement autonome, pas pour les sous-systèmes evolo pas de wireless • TouchGo E310 pour les sous-systèmes evolo pas de wireless
		c-lever compact **Options :** • Wireless • Mobile Access • OSS-SO

	Aperçu du système Composants	
Numéro de produit	**Composant**	**Description**
143x / 153x		Cylindre digital **Options :** • Wireless • Mobile Access • OSS-SO
21 20		Serrure d'armoire • OSS-SO
91 15	 	Lecteur distant Périphérique avec unité de saisie déportée **Options supplémentaires :** • Wireless en cas d'utilisation avec le module d'extension 90 43 (non illustré) • Mobile Access (Bluetooth avec unité de saisie correspondante) • OSS-SO • Couplé au sous-terminal de lecteur compact dormakaba 91 10

	Aperçu du système Composants	
Numéro de produit	**Composant**	**Description**
91 04	 	Lecteur compact **Options :** • Mobile Access NFC uniquement NFC et Bluetooth • OSS-SO • Couplé au sous-terminal de lecteur compact dormakaba 91 10
		Cylindre mécatronique **Options :** • Wireless • OSS-SO
		Solution d'accès boîte aux lettres/commande d'ascenseur • Mobile Access

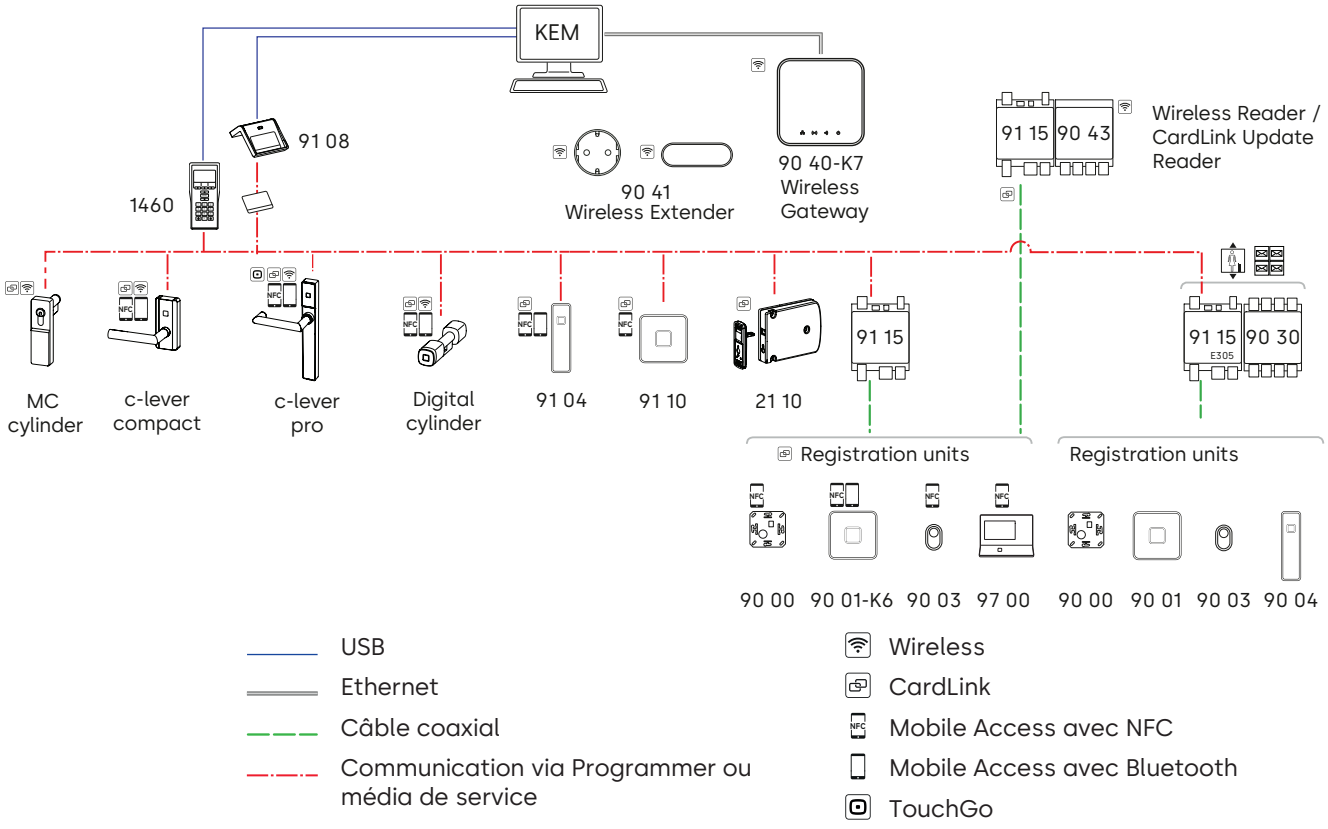
2.3 Logiciel système

Les composants evolo peuvent être configurés avec d'autres logiciels système que dormakaba evolo Manager (KEM).
Des informations sur les possibilités figurent dans la documentation du logiciel système utilisé.

2.3.1 Topologies

Un exemple de topologie possible.

Composants evolo sous KEM :
Édition : 03/2026



Légende				
90 00 90 01 90 03 90 04	Unité de saisie (Registration unit)		91 04 91 10	Lecteur compact
90 40-K7	Hub de communication		91 15 91 25	Lecteur distant
90 41	Wireless Extender		90 30 90 43	Module d'extension
1460	Programmer		91 08	Lecteur de table B-web
91 15 + 90 30	Commande d'ascenseur/boîte aux lettres		91 15 + 90 43	Lecteur wireless Lecteur de mise à jour CardLink wireless

Vous trouverez davantage d'informations sur ces sujets dans les directives de planification pour wireless et Mobile Access.

Mobile Access avec NFC : Mobile Access doit être activé dans le composant.
Mobile Access avec Bluetooth : Le composant dispose du hardware nécessaire pour Bluetooth et Mobile Access est activé dans le composant.

Voir également chapitre [▶ 2.4.1]

2.3.2 Chaîne d'outils

Logiciel système et matériel pour la gestion, la lecture et l'écriture des autorisations dans les composants et les médias.

Aperçu du système Chaîne d'outils	
Outil	**Description**
	Lecteur de table 91 08 MRD Le logiciel système et le lecteur de table permettent de lire et d'écrire les médias.
	Programmer 1460 Le périphérique sert de lien entre les composants autonomes et le logiciel système. Le périphérique est également utilisé pour la configuration initiale/la connexion de composants wireless à un réseau wireless.
	Wireless Gateway 90 40-K7 Le périphérique sert à relier les composants wireless au logiciel système.
	Wireless Extender 90 41 Le périphérique augmente la portée du hub de communication.
	Wireless Reader Connexion wireless pour le lecteur distant 91 15 via un module d'extension wireless 90 32 enfiché. Pour la mise à jour CardLink via wireless.
	Terminal Pour la mise à jour CardLink

2.4 Options d'accès par smartphone

Les utilisateurs peuvent utiliser des applications mobiles ou l'accès par Wallet comme alternative à leurs médias d'accès habituels. Pour plus de détails, voir les chapitres suivants.

2.4.1 Applications Mobile Access

Dans les applications Mobile Access, l'accès s'effectue au moyen des fonctionnalités d'un smartphone. Avec une autorisation d'accès, la serrure/la porte peut être ouverte manuellement. Lorsque l'accès est accordé, un signal visuel et sonore informe l'utilisateur.

Une configuration en parallèle à l'accès conventionnel par médias est possible.

Condition technique préalable pour bénéficier de toutes les fonctions :

Pour pouvoir utiliser Bluetooth, le composant doit être équipé du matériel nécessaire.

- Contrôler les capacités Bluetooth du composant à l'aide du Programmer.

Technologie	Smartphone Système d'exploitation	Composant
NFC	Android	Équipement standard et Mobile Access activé
NFC + BLE	Android iOS	Matériel compatible Bluetooth et Mobile Access activé

Application	Description
App mobile access	Application smartphone pour ouvrir les portes. Média utilisateur
VCP Installer	Application smartphone pour la mise en service des composants de porte (composants evolo, lecteurs d'accès).
evolo smart	Application smartphone pour la mise en service et la gestion des composants de porte. Logiciel système.

Logiciel système

Le logiciel système [▶ 2.3] sert à la gestion du plan de fermeture. Dans les versions actuelles, Mobile Access peut être configuré dans le plan de fermeture. Voir le chapitre Configuration requise du système [▶ 7.6.1].

2.4.2 Accès par Wallet (Apple Wallet et Google Wallet)

Apple Wallet et Google Wallet peuvent être utilisés comme médias utilisateurs sur les composants evolo pris en charge. L'accès est accordé à l'utilisateur via NFC lorsqu'il approche son smartphone du composant. L'application dormakaba n'est pas nécessaire pour cette fonction.

L'accès par Wallet est indépendant de Mobile Access basé sur Bluetooth. Aucune licence Mobile Access supplémentaire n'est requise ; les composants des gammes de produits E300 et E320 suffisent donc.

Conditions requises et restrictions

- Le micrologiciel du composant doit être en version 42.46 ou supérieure (Apple Wallet) ou 42.48 ou supérieure (Google Wallet).
- Si des médias MIFARE sont utilisés dans la même installation, MIFARE DESFire est requis. Les identifiants Wallet ne sont pas compatibles avec MIFARE Classic.
- Le système hôte doit prendre en charge cette fonction. Voir la documentation de configuration du système hôte correspondant.

2.5 Médias

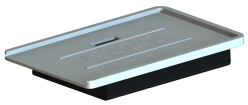
Les médias master n'ont pas d'autorisation d'accès.

Aperçu du système Médias	
Média	**Description**
Médias master	
	Carte master A Cylindre mécatronique clé master A
	Carte master B Cylindre mécatronique clé master B

Aperçu du système Médias	
Média	**Description**
	Carte master T (utilisée uniquement avec KEM)
	Média master TouchGo (RCID, uniquement TouchGo E110)

Les médias utilisateurs sont utilisés avec les autorisations d'accès programmées sur des portes ou dans des groupes de portes.

Aperçu du système Médias	
Média	**Description**
Médias utilisateurs	
	Carte
	Carte avec code QR (evolo smart)
	Cylindre mécatronique
	Porte-clés
	Porte-clés avec code QR (evolo smart)
	Mobile Access L'autorisation d'accès se fait par smartphone. Dans diverses applications, il est également possible de configurer les composants via smartphone. Voir chapitre LIEN [▶ 2.4.1] : Applications Mobile Access
	Porte-clés TouchGo

Aperçu du système Médias	
Média	**Description**
	Bracelet TouchGo
	Porte-carte TouchGo

Médias spéciaux :

Aperçu du système Médias	
Média	**Description**
Cartes de sécurité	
	La carte de sécurité est créée pour chaque installation de fermeture et sert à la sécurité de l'installation. • MIFARE : Carte de sécurité C • LEGIC : Carte de sécurité C1 et C2
Dispositif de test wireless	
	Cela sert, entre autres pour mesurer la portée des composants wireless : Uniquement pour les composants wireless. Vous trouverez d'autres informations dans la directive de planification wireless.
Cartes de licence	
	Upgrade du niveau de système Vous trouverez d'autres informations au chapitre Niveau de système [▶ 3.2].

2.5.1 Médias master

Les médias master permettent d'initier ou de terminer le processus de programmation sur les composants autonomes.

Sans système hôte :

- Après l'initiation du processus, une Whitelist manuelle est configurée.
  Voir le chapitre "Programmer avec des médias".
- Les Master B sont organisés sous un Master A. Vous trouverez des informations sur les structures de programmation au chapitre "Structures de programmation".
- Les médias master n'ont pas d'autorisation d'accès.

Avec système hôte :

Vous trouverez des informations sur l'utilisation des médias master dans la documentation du système hôte utilisé.

- Après l'initiation du processus, un fichier de configuration est chargé à l'aide du Programmer.
  Voir "Programmation avec logiciel système".

Composants wireless :

- Un média master est requis pour pouvoir établir la connexion entre le composant et le hub de communication à l'aide du Programmer.

Master T :
les Master T sont des master temporaires avec une validité restreinte et des fonctions limitées. Les Master T ne sont pas possibles dans tous les systèmes hôtes. Voir la documentation du système hôte utilisé.

TouchGo :
Le TouchGo E110 est uniquement programmable en Whitelist autonome et ne peut pas être utilisé avec un système hôte. La programmation nécessite le Master RCID.

Le TouchGo E310 peut uniquement être utilisé dans un sous-système evolo avec système hôte et chaîne d'outils. Les autorisations RCID et RFID sont configurées dans le logiciel système et associées au composant par pairing. Le média master valide pour le sous-système evolo est utilisé.

Médias



TouchGo



RCID uniquement TouchGo E110

2.5.2 Médias utilisateurs

Les médias utilisateurs permettent aux utilisateurs d'exercer les autorisations qui leur sont attribuées et, par exemple, d'ouvrir des portes.

Sans système hôte
En cas de programmation par Whitelist, les médias utilisateurs sont organisés sous un Master B.

AVIS

Accès non autorisé avec un média perdu

Supprimer le média perdu des composants :

- Annuler toutes les autorisations d'accès avec le Master (les supprimer de la Whitelist), voir chapitre « Annuler toutes les autorisations d'accès attribuées par le Master B ».
- Accorder des autorisations d'accès aux médias utilisateurs toujours valables (les inscrire dans la Whitelist), voir chapitre « Accorder des droits d'accès ».
- Répéter la procédure sur tous les composants auxquels le média perdu a accès.

Avec système hôte

Les autorisations d'accès des médias utilisateurs sont programmées à l'aide de fichiers de configuration. Vous trouverez des informations à ce sujet au chapitre "Programmation avec logiciel système" [▶ 7.5.2].

Médias

RFID

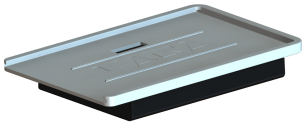




NFC/Bluetooth



TouchGo


Média utilisateur	RCID
Média combiné	RCID + RFID

2.6 Structures de programmation

Uniquement avec programmation autonome sans système hôte.
Uniquement programmation en Whitelist.

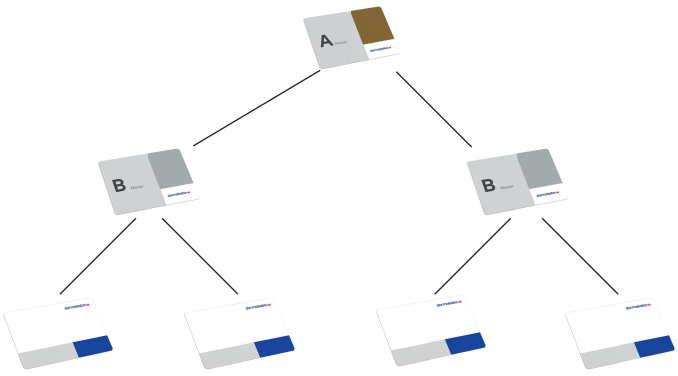
Organisation des composants dans une structure A/B ou une structure B.

La programmation est décrite au chapitre "Programmation avec des médias".

2.6.1 Structure A/B et B

Systèmes basés sur carte :

Structure A/B

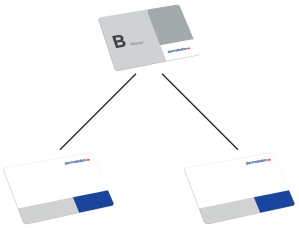


Master A

Master B

Médias utilisateurs

Structure B

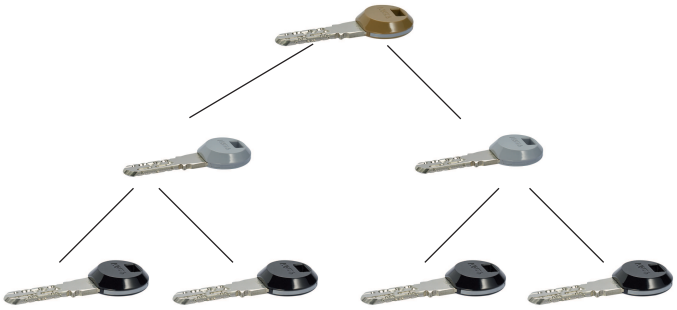


Master B

Médias utilisateurs

Systèmes mécatroniques :

Structure A/B

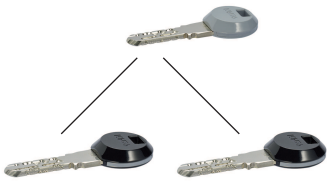


Master A

Master B

Médias utilisateurs

Structure B



Master B

Médias utilisateurs

Description / Exemples

Structure A/B :

Master A :

- Créer un maximum de 200 Master B
- Pas de programmation des médias utilisateurs
- Pas de programmation des autorisations d'accès
- Autres applications, voir les chapitres suivants

Master B :

- Accorder et retirer les autorisations d'accès

Médias utilisateurs :

- 4000 médias utilisateurs au maximum
- La répartition des utilisateurs sur différents Master B peut être effectuée de n'importe quelle manière

Exemple pour 1 composant d'une installation

- Master B1 : 50 utilisateurs
- Master B2 : 3950 utilisateurs

Total = 4000 : Le nombre maximum d'utilisateurs a été atteint.

Structure B :

Master B :

- Accorder et retirer les autorisations d'accès
- Autres applications, voir les chapitres suivants

Médias utilisateurs :

- 4000 médias utilisateurs au maximum

- La répartition des utilisateurs sur plusieurs Master B est **impossible**.

Exemple pour 1 composant d'une installation

- Master B : 4000 utilisateurs

Total = 4000 : Le nombre maximum d'utilisateurs a été atteint.

2.7 Prise en charge d'OSS-SO

OSS-SO (Open Security Standards – Standard Offline) est une norme industrielle ouverte pour le contrôle d'accès hors ligne basé sur carte. Elle permet l'interopérabilité entre les systèmes de contrôle d'accès et les dispositifs de fermeture hors ligne de différents fabricants. Les autorisations d'accès sont enregistrées sur le média utilisateur (Data on Card) et lues directement par le composant. Le composant n'a pas besoin d'être connecté au système hôte.

Les composants evolo peuvent être utilisés sous OSS-SO. La configuration s'effectue à l'aide de la chaîne d'outils OSS-SO et des fichiers XML fournis par le système hôte.

Restrictions

Les fonctions suivantes ne sont pas prises en charge en cas d'utilisation sous OSS-SO :

- Fonctions de commutation S-Module S-Module [▶ 3.9.3]
- Mode Pass Mode Pass avec c-lever pro [▶ 3.9.5]
- Pass-Lock Pass-Lock avec c-lever pro [▶ 3.9.6]

Comportement du cylindre mécatronique en mode Office sous OSS-SO

Le mode Office n'est pas pris en charge sur le cylindre mécatronique. Si le cylindre fait partie d'un groupe d'accès pour lequel des autorisations de basculement (toggle) OSS-SO sont configurées, le composant effectue une ouverture normale au lieu d'activer le mode Office. Ce comportement est identique à celui du fonctionnement sous CardLink.

Pour plus d'informations concernant OSS-SO :

- http://www.oss-association.com/standards/oss-standard-offline/
- Manuel de référence Fichier XML OSS-SO
- Manuel d'utilisation de la chaîne d'outils OSS-SO

3 Types d'autorisations et fonctions

Ce chapitre décrit les deux types d'autorisation Whitelist et CardLink ainsi que les fonctions respectives des composants evolo associés.

- Whitelist : Voir chapitre
- CardLink : Voir chapitre
- AoC : Voir chapitre [▶ 3.5]

3.1 Numéro d'identification

Un numéro d'identification est attribué aux médias et aux composants pour l'autorisation. Ceci est nécessaire pour une identification univoque.

Le numéro unique (UID) est un numéro d'identification unique émis par le fabricant de la carte et enregistré dans les médias utilisateurs. Celui-ci ne peut pas être modifié ou supprimé.

Le Card ID (CID) est un numéro d'identification unique qui peut être attribué par le logiciel système. À l'heure actuelle, ceci n'est possible qu'avec KEM. Des médias avec un CID défini peuvent être commandés. Le CID est enregistré sur le média utilisateur avec la clé du site unique et est lu par les composants de l'installation.

3.2 Niveau de système

Les composants sont livrés au client avec un niveau de système prédéfini. Le niveau de système configuré détermine la compatibilité du composant avec le système hôte utilisé. Les systèmes hôtes fournissent la configuration correspondant au niveau de système qui leur est attribué. Un composant avec un niveau de système inférieur ne peut alors pas être configuré. Un composant avec un niveau de système supérieur peut être utilisé sur un système hôte avec un niveau de système inférieur.

Vue d'ensemble
Vue d'ensemble des systèmes hôtes utilisés et du niveau de système correspondant.

Système	Niveau de système	Définition sur le programmer
		Micrologiciel à partir de 1.30
evolo smart	SL1	1
MATRIX ONE / exivo / KEM	SL2	2
MATRIX PRO / exos / EACM	SL3	3
OSS (tiers + hôte dormakaba)	SL4	4

Le niveau de système d'un composant peut être déterminé à l'aide du Programmer.

Déterminer l'état du niveau de système et « BLE ready ».
Sélectionner le menu « Information actuateur » dans le programmer et lire les informations du composant.

Conditions requises :

- Programmer 1460
- Média master du composant

Marche à suivre :

1. S'enregistrer au composant avec le média master.
2. Sélectionner le menu Lire l'actuateur.
3. Sélectionner l'entrée de menu 'Info'.
4. Connecter le programmer au composant.

Déterminer la variante (E3xx) et la version du micrologiciel.

Le niveau de système est spécifié sous SL.

Sous BLE, un champ coché indique que BLE est actif.

Le niveau de système est pris en charge par les composants et les systèmes hôtes à partir des versions suivantes.

Le composant ne peut être configuré que si les niveaux de système du composant et du fichier de configuration correspondent.
Le composant peut être configuré si son niveau de système est supérieur au niveau de système du système hôte (s'applique à SL1 jusqu'à SL3. Ne s'applique pas à SL4).

Une mise à jour du micrologiciel est possible même si le niveau de système est incorrect.

Système hôte	à partir de la version	Remarques
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	Le programmer compare le niveau de système du fichier de paramètres au niveau de système du composant.
Composant (version du micrologiciel)	42.28	En usine, le niveau de système est réglé après la commande.

Upgrade vers un niveau de système supérieur
Les composants sont expédiés départ usine avec le niveau de système commandé. Si des fonctions qui ne sont pas activées dans ce niveau de système doivent être utilisées, le niveau de système du composant doit être mis à jour au niveau nécessaire. Pour cela, des médias d'upgrade peuvent être achetés.



Les médias suivants sont proposés pour l'upgrade/l'obtention d'une nouvelle licence :

Mise à niveau	SL1 vers SL2
Mise à niveau	SL2 vers SL3
Mise à niveau	SL1 vers SL3
Licence	Mobile Access via BLE

Le processus d'upgrade est consigné dans le manuel technique du composant.

3.3 Autorisation Whitelist

Une autorisation Whitelist représente la quantité de médias autorisés enregistrés dans le composant.

L'autorisation Whitelist est programmée dans les composants.
Cela signifie que l'UID ou la Card ID (CID) du média à autoriser est enregistré dans les composants et donc inscrit dans la Whitelist.

La Whitelist compare l'UID ou le CID des médias présentés. S'il y a des concordances, les médias sont autorisés et les composants s'ouvrent. Jusqu'à 4 000 entrées sont possibles dans la Whitelist. L'UID ou le CID peuvent être entrés.

Exemple de fonctionnement

L'autorisation d'accès n'est accordée que si des médias utilisateurs dont l'UID ou le CID sont enregistrés dans les composants sont présentés.

Composants	Médias	Accès
Liste des UID enregistrés dans les composants	**UID des médias présentés**	
570AE209	570AE209	✓
222BE121	222BE121	✓
—	878EAE964	✗
—	121AC001	✗

3.3.1 Autorisation Whitelist avec profil de temps

Les profils de temps permettent de définir les horaires auxquels des médias sont autorisés pour un composant.

Tous les composants evolo possèdent leur propre heure (Real Time Clock). Il est ainsi possible d'accorder aux médias utilisateurs des autorisations d'accès temporelles, par composant et par porte.

Outre l'autorisation d'accès de base, il est possible de limiter une autorisation dans le temps grâce aux profils de temps. Les profils de temps sont définis dans le logiciel système.

3.3.1.1 Autorisation Whitelist avec profil de temps individuel

Au total, 15 profils de temps sont disponibles par composant, avec chacun 12 plages horaires.

3.3.1.2 Autorisation Whitelist avec profil de temps « Toujours » non modifiable

Ce profil de temps est défini sur l'état « Toujours » et assure l'ouverture 24 heures sur 24, 7 jours sur 7. Le profil de temps « Toujours » ne peut pas être modifié, renommé ou effacé.

3.3.1.3 Congés/jours particuliers

Jours particuliers disponibles :

Profil horaire V4	Dispose de deux jours particuliers A et B

Indication : Lorsque des composants sont mis à jour à l'aide du Programmer 1460, les jours fériés et jours particuliers les plus récents (du jour même et à l'avenir) du logiciel système sont appliqués.

Profils horaires pour les congés
Pour des périodes de jours consécutifs (par exemple, des congés), l'autorisation d'accès peut être accordée ou révoquée. La durée d'une période est définie en entrant les dates de début et de fin. Plusieurs blocs de congés peuvent être créés. Dans les composants (V4), il est possible de définir jusqu'à 20 blocs de congés.

Remarque sur la représentation des jours particuliers dans les blocs de congés : Si des jours particuliers sont situés dans un bloc de congés, ils sont privilégiés dans la représentation, ce qui signifie que la représentation du jour particulier se superpose à la représentation du bloc de congés. Si le jour particulier est supprimé, le bloc de congés s'affiche à nouveau complètement.

Plage horaire pour les jours particuliers

Pour les jours particuliers (par exemple, les jours fériés), il est possible de créer 2 jours différents, jour particulier A et jour particulier B. Ceci permet de créer deux plages horaires, par exemple une plage horaire pour un jour précédant un jour férié (jour particulier A) et pour le jour férié (jour particulier B). Pour chacun des 2 types de jours particuliers, un total de 32 jours particuliers peut être enregistré dans les composants.

Types de jours particuliers	Jour particulier	Nombre Nombre de jours particuliers dans le composant
Jour particulier A	Jour avant un jour férié	32
Jour particulier B	Jour férié	32

3.3.1.4 Heure d'été/hiver

Dans les composants, le passage à l'heure d'été/hiver est effectué automatiquement selon le fuseau horaire mondial défini, en fonction du logiciel système utilisé.

3.4 Autorisation CardLink

Pour le type d'autorisation CardLink, l'autorisation d'accès est gérée via les médias utilisateurs. Cela élimine le travail administratif local sur les composants. Pour ce type d'autorisation, les applications médias sur les médias utilisateurs sont nécessaires.
Lors de la mise en service, les composants doivent être programmés une seule fois.

Ce type d'autorisation permet également la validation (activation pendant un certain temps – Validation [▶ 3.4.2]) des médias utilisateurs pour l'autorisation d'accès aux composants autonomes.

Avantages

- L'autorisation d'accès est écrite directement dans les médias utilisateurs.
- L'autorisation peut être limitée dans le temps via la fonction **Réservation**.
- Il est possible d'attribuer une sélection individuelle de portes ou de groupes de portes à un visiteur sur un média utilisateur.
- Aucune configuration supplémentaire n'est requise sur les composants pour des médias utilisateurs supplémentaires.
- La création supplémentaire de groupes simplifie la structure des installations de fermeture et l'attribution des autorisations.

3.4.1 Droits d'accès

Une autorisation unique et temporisée est attribuée aux médias utilisateurs pour une sélection de composants ou de groupes de portes. Pour cela une liste de groupes de portes ou de portes est enregistrée dans les médias utilisateurs.

Droit de groupes de portes
Les droits groupe de portes peuvent être regroupés de manière organisationnelle (par personnes) ou spatiale (par parties du bâtiment).

Un droit groupe de portes est une autorisation d'accès avec un profil de temps parent. Pour un droit de groupe de portes, plusieurs personnes ou portes sont regroupées dans un groupe de portes. Le groupe de portes est enregistré en tant qu'identification dans les composants et un profil de temps est attribué au groupe de portes. Ce groupe de portes peut ensuite être attribué aux médias utilisateurs, ce qui permet l'accès à toutes les portes affectées à ce groupe de portes.
Pour l'autorisation CardLink, 15 profils de temps avec respectivement 12 plages horaires sont disponibles, ainsi que le profil de temps « Toujours », qui est toujours valide. Chaque groupe de portes peut se voir attribuer un profil de temps correspondant.

Applications :

- Pour les installations de fermeture de grande taille avec de nombreux utilisateurs et un grand nombre de portes. La configuration de groupes de portes permet de mieux structurer et de mieux gérer les installations de fermeture.
- Pour un groupe de personnes qui ont besoin des mêmes autorisations d'accès pour un groupe de portes que les chefs de groupes et les concierges.

Droit individuel
Un droit individuel est une autorisation d'accès avec un profil de temps individuel, valable pour une porte individuelle ou un groupe de portes.

Le profil de temps d'un droit individuel est enregistré sur les médias utilisateurs. Dans le cas d'un droit individuel, le profil de temps peut être sélectionné individuellement pour le groupe de portes (Droit groupe de portes).

2 variantes sont disponibles :

1 Droit individuel pour portes individuelles
Une autorisation d'accès avec des profils de temps individuels peut être attribuée aux médias utilisateurs pour une porte.

2 Droit individuel pour groupe de portes
une autorisation d'accès avec des profils de temps individuels peut être attribuée aux différents utilisateurs (à leurs médias utilisateurs) pour un groupe de portes.

Applications :

- Pour des installations de fermeture de petite taille avec peu d'utilisateurs et un nombre restreint de portes.
- Pour plusieurs utilisateurs ayant besoin d'une autorisation d'accès individuelle à des portes individuelles, comme le personnel de nettoyage et de sécurité.
- Pour les utilisateurs individuels ayant besoin d'une autorisation d'accès individuelle pour un groupe de portes, comme les chefs de groupes et les concierges.

Réservation

Une réservation est une autorisation d'accès pour les visiteurs au même titre que les droits individuels, mais avec en plus des dates de début et de fin ou une durée de validité.

Applications :

- La réservation est une autorisation temporaire qui est utilisée pour les clients, les visiteurs et les fournisseurs.

Priorisation des droits

Les droits sont priorisés. En priorisant les droits, l'autorisation d'accès d'un média peut être restreinte ou étendue.

Les droits sont traités dans l'ordre suivant.

- Droit individuel
- Réservation
- Droit de groupes de portes

L'évaluation du droit suivant ne sera poursuivie que si aucun droit « temporellement incorrect » n'est constaté. Si un droit « temporellement incorrect » est constaté, la vérification est immédiatement interrompue.

Lors de l'évaluation du droit groupe de portes, cependant, la recherche continue jusqu'à ce que :
a) tous les droits soient contrôlés ou b) un droit valide (groupe de portes et profil de temps approprié) soit trouvé.

Exemple de fonctionnement

Voici quelques exemples des différents droits d'accès.

Les conditions sont les suivantes :

- Groupe de portes A --> Profil de temps 1
- Plusieurs composants --> Groupe de portes A
- Porte « Entrée » --> Profil de temps 1 à 15

Exemple de droits d'accès :

Droits d'accès	Média avec données	Accès pour	
		Groupe de portes A	Porte « Entrée »
Droit de groupes de portes	Groupe de portes A	✓ durant profil de temps 1	✗
Droit individuel du groupe de portes A	Groupe de portes A + Profil de temps 4	✓ durant profil de temps 4	✗
Droit individuel de la porte	« Entrée » + Profil de temps 3	✗	✓ durant profil de temps 3

Droits d'accès	Média avec données	Accès pour	
Réservation du groupe de portes A	Groupe de portes A + Profil de temps 2 du démarrage à l'arrêt	✓ durant profil de temps 2 du démarrage à l'arrêt	✗
Réservation de la porte	« Entrée » + Profil de temps 7 du démarrage à l'arrêt	✗	✓ durant profil de temps 7 du démarrage à l'arrêt
Combinaison entre droit de groupes de portes et Droit individuel	Groupe de portes A « Entrée » + Profil de temps 3	✓ durant profil de temps 1	✓ durant profil de temps 3

3.4.2 Validation

La validation (jeton d'horodatage sur les médias utilisateurs) est une activation d'une autorisation d'accès. L'accès n'est possible que si une autorisation CardLink valable est présente et que la durée de la validation [▶ 3.4.3] est activée.

Avantages

- Les médias utilisateurs perdus peuvent être rapidement et facilement bloqués par la validation.
- L'autorisation CardLink expire à l'issue de la durée de la validation. L'autorisation d'accès et la validation expirent alors. La validation ne peut plus être remplacée.

3.4.3 Valider les médias

Validation avec des composants autonomes

Les composants autonomes peuvent également être utilisés comme composants de validation. Les composants de validation peuvent être configurés pour la validation de l'autorisation CardLink. Si la validation est modifiée, les composants doivent être actualisés à l'aide du Programmer 1460 ou via wireless.

Étant donné que la validation nécessite davantage d'énergie, il est recommandé d'utiliser uniquement des composants dotés d'une alimentation électrique externe. Les lecteurs remote, les lecteurs compacts ou c-lever avec S-Module sont appropriés.

Validation avec lecteur de mise à jour wireless

Les médias utilisateurs peuvent être validés sur un ou plusieurs lecteurs de mise à jour wireless. En même temps, la validation ou l'autorisation d'accès de médias utilisateurs perdus peut y être révoquée. Les données de validation sont gérées par le logiciel système et transmises via wireless au lecteur de mise à jour.

Validation avec terminal

Les médias utilisateurs peuvent être validés sur un ou plusieurs terminaux de validation. En même temps, la validation ou l'autorisation d'accès de médias utilisateurs perdus peut être révoquée directement sur un terminal. Le terminal est géré par le logiciel système.

Durée de la validation

Avec la validation sur un terminal ou un composant de validation, un jeton d'horodatage est inscrit sur les médias utilisateurs. L'autorisation d'accès pour les composants autonomes CardLink est valable à partir de cette date.

La durée de validité des médias est vérifiée lors de la présentation des médias utilisateurs. Cela signifie que l'accès n'est accordé que si la durée de validité n'a pas expiré et si l'autorisation temporaire pour la porte ou le groupe de portes correspondant (conformément au profil de temps) existe.

Les types de validations suivants peuvent être utilisés :

Types de validation	État
Durée en jours et en heures	En jours et en heures (valeur maximale 999 j et 24 h)
24 heures (1 jour)	Le type n'est pas modifiable.
Heure de fin (h)	Jusqu'à une certaine heure de la journée.
« toujours »	Le type n'est pas modifiable.

Pour le type de validation « Toujours », les médias utilisateurs perdus ne peuvent plus être désactivés. Pour cette raison, les médias utilisateurs perdus doivent impérativement être inscrits sur la Blacklist [▶ 3.4.5] des composants pour une durée illimitée.
L'espace d'enregistrement pour l'entrée de médias perdus dans la Blacklist est limité.
Il n'est pas recommandé d'utiliser ce type de validation.

Modes de validation
Dans les modes de validation, on distingue le type de média et le type de composant. Le mode de validation est toujours réglé sur le composant. Les deux modes de validation peuvent être mis en œuvre dans une installation de fermeture.

Type de média (standard)
La durée de la validation est créée par défaut sur tous les médias utilisateurs. Lors de la présentation des médias utilisateurs aux composants, le jeton d'horodatage actuel et la durée de la validation des médias utilisateurs sont lus et comparés à l'heure actuelle du composant. Si l'heure actuelle est antérieure au jeton d'horodatage et à la durée, la validation est valide. Si l'heure actuelle est postérieure, l'heure de validation est considérée comme écoulée et le média comme invalide.

Type de composant
La durée de la validation est enregistrée sur les composants. Lors de la présentation de médias utilisateurs à des composants, seul le jeton d'horodatage actuel des médias utilisateurs est lu et comparé à l'heure actuelle des composants. Si l'heure est comprise dans la durée de la validation, l'autorisation des médias utilisateurs est valide. Si l'heure est postérieure, l'heure de validation est considérée comme écoulée et le média n'est plus valide, ni autorisé.

Les types de validation suivants sont possibles :

Modes de validation	Durée de la validation déterminée par	Jeton d'horodatage à actualiser
Médias (standard)	Médias	sur les médias
Composants	Composants	sur les médias

Exemple de fonctionnement
Dans une installation de fermeture, la durée de validation choisie enregistrée dans les médias utilisateurs est de 48 heures. À chaque accès à l'entrée principale, les médias utilisateurs sont actualisés et obtiennent l'accès aux portes du bâtiment. Les employés en voiture utilisent le parking extérieur, sécurisé par une barrière. Comme la validation ne peut pas être effectuée au composant de la barrière, les validations de 48 heures ne sont plus valides après les week-ends ou les vacances. La barrière resterait fermée. Dans ce cas, la barrière peut être configurée avec validation des composants. Celle-ci permet de paramétrer une durée de validation de 4 semaines. Cela garantit que la barrière s'ouvrira également avec un jeton d'horodatage datant de 3 semaines.

3.4.4 Médias perdus

La validation n'est plus renouvelée pour des médias utilisateurs perdus. Les médias deviennent invalides et l'accès est verrouillé.

Il existe 4 possibilités d'exclure des médias perdus :

- Pour les terminaux, l'état du média est défini comme « Perdu » dans le logiciel système et n'est ensuite plus validé par le terminal.
- Pour les composants de validation, le média est inscrit dans la Blacklist. Le média perdu ne peut plus être validé. Cependant, le média devient invalide seulement après écoulement de la durée de la validation.
- Lors du fonctionnement avec des composants autonomes, le média est inscrit dans la Blacklist. Les données sont ensuite transférées à tous les composants autonomes de l'installation en question via le programmer, un média de service ou, le cas échéant, via une connexion wireless.
- En cas de fonctionnement avec des composants wireless, un nouveau paramétrage est transféré aux composants dans le logiciel système après que le média perdu ait été rayé.

3.4.5 Liste noire

La fonction Blacklist permet de bloquer des médias utilisateurs sur tous les composants (de validation) autonomes.

Si des médias utilisateurs doivent être bloqués pendant la durée de validité d'une validation, ce blocage doit être effectué avec le Programmer 1460 ou un média de service sur tous les composants autonomes de l'installation en question. La reconfirmation peut ensuite être transférée au logiciel système à l'aide du Programmer 1460 ou du média de service correspondant.

Le blocage peut également être effectué via la chaîne d'outils logiciel système -- Programmer ou via wireless.

3.4.6 Médias de service

Les médias de service sont uniquement possibles sous KEM.

Avant de pouvoir utiliser des médias comme médias de service, ces médias doivent être définis comme tels à l'aide du logiciel système. Pour cela, des cartes de fonction identifiables comme telles par leur maquette sont disponibles.



Les médias utilisateurs perdus peuvent être entrés dans la Liste noire [▶ 3.4.5] à l'aide du logiciel système. Cette entrée dans la Blacklist est écrite sur le média de service et transférée aux composants via ce média. La reconfirmation s'effectue en faisant lire à nouveau le média de service par le logiciel système.

3.4.7 Information sur l'état

Les informations d'état sont des informations additionnelles qui sont transférées par le composant sur les médias. Lorsque la puissance des piles dans un composant atteint un niveau trop faible, cette information d'état est écrite sur les médias. Lorsque des médias avec ces informations d'état sont lus par un lecteur de table ou un terminal, l'information est transmise au logiciel système et y est affichée.

Pour les composants wireless, les informations d'état sont transmises sans fil au logiciel système et y sont affichées. Si nécessaire, le processus doit être lancé dans le logiciel système.

3.4.8 Traceback des médias

La fonction peut être configurée dans le logiciel système.

Dans le type d'autorisation CardLink, il est possible d'enregistrer des événements d'accès spécifiques aux médias sur les médias utilisateurs. Ces données peuvent être lues par un lecteur de table ou un terminal et transférées au logiciel système.

Par exemple, les événements et états suivants sont enregistrés :

- Accès avec autorisation

- Accès refusé
- Validation invalide
- Mauvais moment

3.5 Access on Card

En mode Access on Card (AoC), les autorisations sont enregistrées sur le média utilisateur. Les données d'accès comportent une durée de validité qui peut varier selon les besoins de l'utilisateur. La durée de validité peut également être définie comme illimitée, c'est-à-dire sans date d'expiration. Le mode AoC est défini dans l'environnement MATRIX.

Avec Data on Card, les données du composant sont enregistrées sur le média utilisateur lors d'une saisie. Ces données sont lues par un lecteur connecté à un système hôte en vue de leur traitement dans le système hôte.

3.6 Mode mixte

En mode mixte, les autorisations sont enregistrées sur un média CardLink ou une Whitelist. Si le média d'un composant configuré en mode mixte est présenté, le composant vérifie d'abord s'il y a une autorisation Whitelist. S'il ne trouve aucune autorisation, une vérification par rapport aux autorisations CardLink est effectuée. Le composant s'ouvre si le média est autorisé dans l'un de ces types d'autorisation.

Si le média est trouvé pour les deux types d'autorisation et que le média est classé comme « pas autorisé » dans un type d'autorisation, le média est refusé.

Exemple : Le composant ne s'ouvre pas si une autorisation CardLink valide existe pour un média, mais que ce dernier dispose également d'une autorisation Whitelist avec un profil de temps non valide.

3.7 Médias non autorisés

Les composants restent fermés lorsque des médias utilisateurs non autorisés sont présentés. Lorsque des médias utilisateurs non autorisés sont présentés à l'état ouvert, les composants restent ouverts. Les composants signalent que les médias non autorisés ne sont pas acceptés.

3.8 Fonctions TimePro

Ce chapitre décrit les fonctions Office et Day/Night de TimePro.

Des informations détaillées et complémentaires sur les deux fonctions TimePro et leurs propriétés pour les composants électroniques sont décrites dans le mode d'emploi du logiciel système KEM.



Avec la c-lever et la c-lever pro, les fonctions TimePro et les fonctions suivantes ne peuvent pas être combinées entre elles :

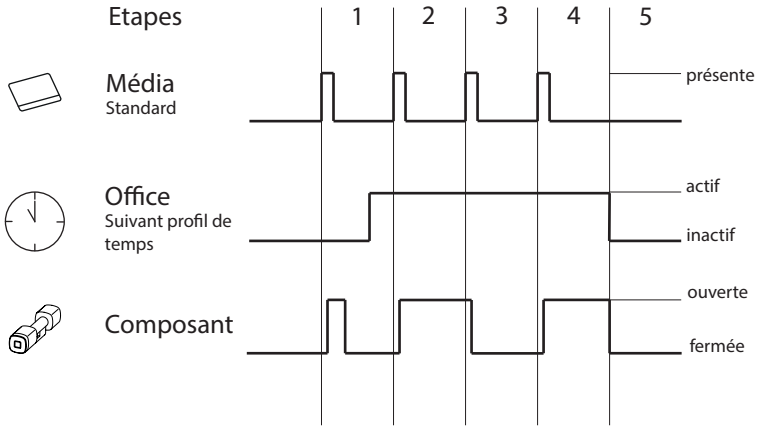
- Mode Pass
- escape return

3.8.1 Profil de temps Office

Dans le profil de temps TimePro saisi, les composants peuvent être mis en état ouvert par des médias autorisés.

Indication : la fonction Profil de temps Office peut être limitée à des médias utilisateurs individuels dans le logiciel système.

Exemple de fonctionnement



Processus 1
Les composants fermés peuvent être ouverts avec des médias utilisateurs autorisés. Après un certain temps d'ouverture (de quelques secondes), les composants se referment automatiquement.

Processus 2
Une fois que des médias utilisateurs autorisés ont été présentés, les composants restent ouverts en permanence.

Processus 3
Lorsque des médias utilisateurs autorisés sont présentés lors de l'état ouvert, les composants se referment à nouveau.

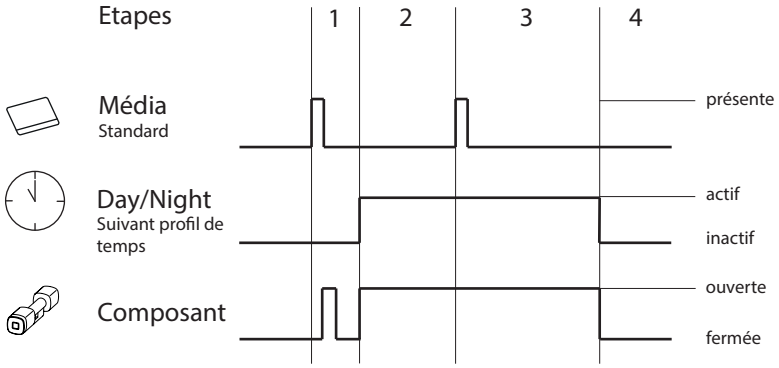
Processus 4
Une fois que des médias utilisateurs autorisés ont été présentés une nouvelle fois, les composants restent ouverts en permanence.

Processus 5
Lorsque le profil de temps Office a expiré, les composants se ferment automatiquement.

3.8.2 Profil de temps Day/Night

Le profil de temps Day/Night détermine l'intervalle au cours duquel les composants sont à l'état ouvert.

Exemple de fonctionnement



Processus 1

Les composants fermés peuvent être ouverts avec des médias utilisateurs autorisés. Après un certain temps d'ouverture (de quelques secondes), les composants se referment automatiquement.

Processus 2

Au démarrage du profil de temps, les composants s'ouvrent automatiquement.

Processus 3

Pendant l'état ouvert des composants, les médias autorisés ou non autorisés n'ont aucune influence sur l'état des composants. Les composants restent ouverts et émettent des signaux, comme c'est le cas pour les médias avec autorisation d'accès.

Processus 4

Une fois le profil de temps écoulé, les composants se referment automatiquement.

Exemple de fonctionnement

L'autorisation d'accès n'est accordée que si des médias utilisateurs dont l'UID ou le CID sont enregistrés dans les composants sont présentés.

Exemple de fonction Whitelist avec profil de temps :

Composants	**Médias**	**Accès**
Liste des UID enregistrés dans les composants et des profils de temps associés	**UID des médias présentés pendant un certain temps**	
	Exemple : Vendredi 5 août 2014 / 10h15	
578AE976 « toujours »	578AE976	✓
222BE121 Lundi – Vendredi 8h00 – 17h00	222BE121	✓
829FE649 Dimanche 10h00 – 12h00	829FE649	✗
—	121CA001	✗

3.9 Fonctions avancées

3.9.1 Composants wireless

Avec la fonction wireless, les composants autonomes sans fil V4 sont connectés par radio au logiciel système correspondant.

La fonction wireless est une option pour les composants autonomes V4 (MRD), comme le cylindre digital et la béquille électronique c-lever. L'option est configurée avec le logiciel système, par exemple KEM.

Avantages

- Frais d'administration et de gestion réduits
- Modification des autorisations d'accès en temps réel
- Interrogation et enregistrement directs des événements et états
- Affichage de l'état des piles
- Transfert des mises à jour du micrologiciel par radio

Restrictions :

- Cette fonction ne peut pas être combinée avec TouchGo.

3.9.1.1 Vue d'ensemble

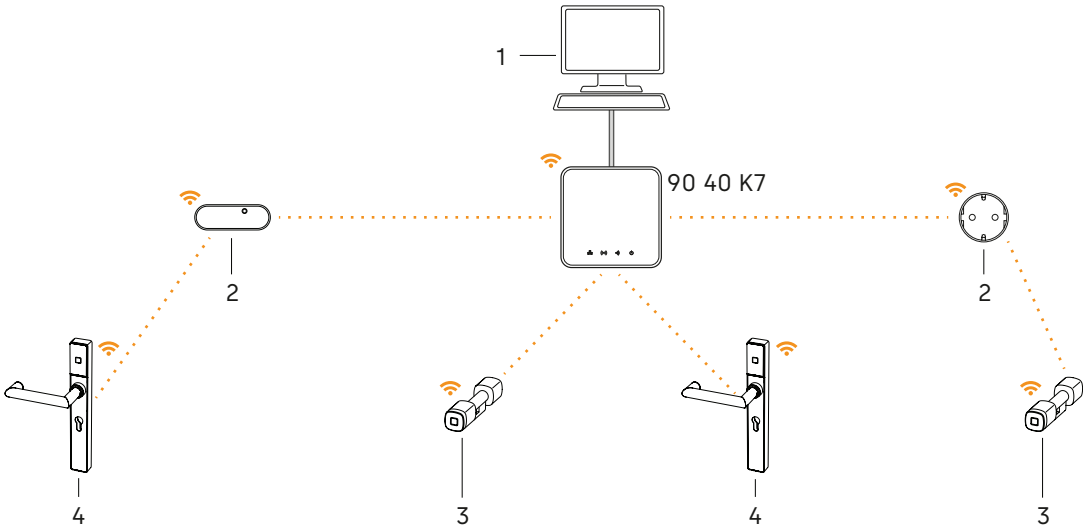
Le hub de communication permet de connecter des composants wireless à un système de contrôle d'accès.

Le système de contrôle d'accès est géré grâce à un logiciel système. Le logiciel système permet de configurer les périphériques connectés et d'attribuer les droits d'accès.

La transmission de données au logiciel système s'effectue via la ligne Ethernet. La transmission de données aux composants wireless s'effectue par radio.

La portée de la connexion radio peut être étendue avec des Wireless Extender.

Topologie
Le graphique montre l'intégration de la wireless gateway dans un système dormakaba avec des composants wireless et des Wireless Extenders.



Périphérique wireless
Communication wireless

1 Système parent
2 Wireless Extender
3 Composant wireless (cylindre digital)
4 Composant wireless (c-lever pro)

1 Logiciel système

2 Hub de communication

3 Composant de porte wireless

– Il est possible de connecter 16 composants de porte wireless max. à un hub de communication.

4 Wireless Extender

– Il est possible de connecter 8 Wireless Extender max. à un hub de communication.

– Il est possible de connecter 4 Wireless Extender max. en série.
(Hub de communication → 1. Wireless Extender→ ... → 4. Wireless Extender)

3.9.1.2 Mesure avec l'outil Site Survey Tool

Le Site Survey Tool permet de mesurer la qualité du signal d'un hub de communication en différents points. Les résultats des mesures permettent de déterminer la position de la passerelle réseau de manière à ce que tous les composants wireless bénéficient d'une qualité de signal optimale. Si la qualité du signal n'est pas suffisante pour un fonctionnement sécurisé, il faut alors ajouter d'autres passerelles réseau ou répétiteurs au système.

Pour de plus amples informations, consulter la directive de planification wireless et la description du programme concernant Site Survey Tool.

3.9.1.3 Mesure de la portée avec un média de test wireless

Méthode de mesure alternative si l'outil Site Survey Tool n'est pas disponible.

Vous trouverez une description détaillée de la mesure de la portée avec la passerelle réseau dans les instructions séparées PG Wireless (directives de planification) et dans le manuel du hub de communication.

Média requis : dispositif de test wireless



3.9.1.4 Mise en service

La mise en service des composants wireless à l'aide du Programmer 1460 est décrite dans les manuels du Programmer, du hub de communication et du logiciel système.

Principe
La mise en service wireless est lancée sur le hub de communication 90 40-K7 auquel le composant doit se connecter. Le Programmer permet de lancer la séquence de connexion sur le composant. Une fois le composant connecté avec succès au hub de communication, il peut être configuré en ligne à l'aide du logiciel système.

3.9.2 Traceback de composants

Le Traceback de composants est un fichier journal dans lequel tous les événements des composants sont saisis et enregistrés. La fonction peut être désactivée dans le logiciel système.

Jusqu'à 2 000 événements sont enregistrés dans la mémoire. L'entrée la plus récente écrase l'entrée la plus ancienne. Chaque entrée contient un jeton d'horodatage. Pour cela, l'heure du composant doit être réglée correctement. Grâce aux logs, tout accès autorisé ou refusé à une porte peut être retracé.

Par exemple, les événements et états suivants sont enregistrés :

- Accès avec autorisation
- Accès refusé en raison d'autorisation ou de validation manquante
- Accès refusé en raison de la plage horaire erronée
- Régler l'heure
- Programmation
- Test du système, etc.

3.9.3 S-Module

Avec le S-Module, le comportement du composant (autorisation) est surcontrôlé par un contact externe sans potentiel. Le S-Module est activé par un interrupteur, une minuterie ou le système de contrôle du bâtiment (par exemple, un système d'alarme). Un composant avec S-Module peut être alimenté en tension par un bloc d'alimentation externe. Dans ce cas, des piles ne sont plus nécessaires.

Le module S est possible pour les composants suivants :

c-lever pro	configurable/peut faire l'objet d'une mise à niveau
Cylindre MC	peut faire l'objet d'une mise à niveau
Gestionnaire de porte	disponible de manière standard
Lecteur compact	disponible de manière standard

Le module S est configuré à l'aide du logiciel système.

Restrictions :

- La combinaison de fonctions de commutation S-Module, Passlock et mode Pass est impossible.
- L'alimentation en tension externe du périphérique est possible avec le S-Module.
- La fonction n'est pas prise en charge lors d'une utilisation sous OSS-SO.

3.9.4 Fonction Retour (Escape Return) avec la c-lever pro

La fonction Escape-Return assure un retour sans entrave et sans média dans les locaux quittés en cas d'urgence (p. ex. incendie).
En effet, pour le cas où une personne quitterait le local sans média, le local n'est pas verrouillé. Le local est verrouillé lorsqu'une personne en sort avec le média ou suite à l'actionnement de la touche.

Restrictions :

- La fonction peut uniquement être utilisée avec des composants c-lever pro.
- La fonction ne peut pas être utilisée avec les fonctions TimePro et Pass-Lock.
- La combinaison de fonctions de commutation S-Module et de la fonction Retour est impossible.
- L'alimentation en tension externe du périphérique est possible avec le S-Module.

3.9.5 Mode Pass avec c-lever pro

Le mode Pass est une option pour la garniture électronique c-lever pro. La fonction est activée et désactivée via une touche. En actionnant la touche (aucun média utilisateur requis), la porte reste ouverte. En appuyant de nouveau sur la touche ou en présentant un média utilisateur autorisé, la garniture électronique de la porte se remet en état fermé. L'état

actuel de la porte peut être consulté à tout moment en actionnant brièvement la touche.
Si le hardware est reconnu, des réglages préconfigurés sont chargés.
Le mode Pass est configuré à l'aide du logiciel système.

Restrictions :

- La combinaison de fonctions de commutation S-Module, Passlock et mode Pass est impossible.
- L'alimentation en tension externe du périphérique est possible avec le S-Module.
- La fonction n'est pas prise en charge lors d'une utilisation sous OSS-SO.
- L'utilisation du mode Pass via wireless est prise en charge à partir de la version du micrologiciel 42.38.

3.9.6 Pass-Lock avec c-lever pro

Pass-Lock est une option pour la garniture électronique c-lever pro. Cette fonction est activée à l'aide de la touche située sur la garniture. Lorsque la touche est actionnée, la porte reste fermée pour les personnes venant de l'extérieur. La présentation d'un média autorisé (master ou utilisateur) remet la c-lever pro à l'état ouvert. La porte peut toujours être ouverte de l'intérieur.
Pass-Lock est configuré à l'aide du logiciel système. Afin d'éviter une activation involontaire, un délai de 0,1 à 5 secondes peut être configuré. Pass-Lock ne s'active que si la touche est maintenue enfoncée pendant toute la durée du délai configuré.

Restrictions

- La combinaison des fonctions de commutation S-Module, Pass-Lock et mode Pass est impossible.
- L'alimentation en tension externe du périphérique est possible avec le S-Module.
- La fonction n'est pas prise en charge en cas d'utilisation sous OSS-SO.
- L'utilisation de Pass-Lock via wireless est prise en charge à partir de la version 42.38 du micrologiciel.
- Le délai d'activation est configurable dans le logiciel système. Si aucun délai n'est configuré explicitement, le comportement par défaut (pas de délai) s'applique. Cette option est disponible à partir de la version 42.48.

3.9.7 Médias d'intervention

Cette fonction est disponible à partir de la version 42.48 du micrologiciel.

Les composants evolo prennent en charge un modèle d'autorisation à deux niveaux (2LA). En plus du groupe standard d'utilisateurs autorisés, un second groupe de médias, défini séparément, peut se voir attribuer des autorisations étendues pour des situations d'accès spécifiques. Ce groupe d'intervention fonctionne indépendamment de l'autorisation standard et peut obtenir l'accès dans des situations où les médias utilisateurs normaux sont restreints ou bloqués, par exemple lorsque Pass-Lock est actif ou lorsqu'un système de détection d'intrusion (IDS) est armé. Les cas d'utilisation suivants sont pris en charge :

Médias d'intervention pour Pass-Lock
Lorsque Pass-Lock est actif, une porte n'est normalement remise à l'état ouvert que par la présentation d'un média master ou de tout média utilisateur autorisé. Un groupe dédié de médias d'intervention peut être configuré à cet effet. Contrairement à tous les autres utilisateurs autorisés, seuls les membres de ce groupe sont alors autorisés à désactiver Pass-Lock. Cette solution est utile lorsque l'on souhaite limiter les personnes habilitées à lever un verrouillage, par exemple au personnel de sécurité ou au personnel technique désigné.

Médias d'intervention pour IDS
Lorsqu'un système de détection d'intrusion (IDS) est armé, tous les médias sont normalement refusés jusqu'à ce que l'IDS soit désarmé. Un groupe spécial de médias d'intervention peut être défini pour conserver l'accès même lorsque l'IDS est armé. Cela permet à des personnes désignées, par exemple les services d'urgence, d'accéder aux locaux quel que soit l'état de l'alarme.

Restrictions

- Les médias d'intervention pour IDS ne sont pris en charge qu'en mode wireless et nécessitent un Wireless Gateway 90 40-K7 avec la version de micrologiciel 5.1 ou supérieure.

- L'armement de l'IDS est une fonction MATRIX. Pour plus de détails sur la configuration, voir la documentation du système hôte MATRIX.
- Les médias d'intervention sont configurés à l'aide du logiciel système. Pour plus de détails sur la configuration, voir le manuel du logiciel système.

3.9.8 Désactiver la programmation manuelle

La programmation manuelle des composants avec des médias est désactivée en cas d'utilisation du logiciel système et du Programmer 1460.

3.10 TouchGo

Le système de fermeture électronique TouchGo est un système d'autorisation d'accès qui peut être utilisé comme installation indépendante ou comme extension confortable du sous-système dormakaba evolo. La technologie RCID constitue la base de ce confort. Voir le chapitre Aspects de sécurité [▶ 3.10.2].

Le système TouchGo est disponible en deux variantes différentes. Celles-ci définissent l'étendue des fonctions des composants. En combinaison avec un sous-système evolo, seuls des composants de la variante TouchGo E310 sont utilisés.

Un système TouchGo permet d'ouvrir des portes sans être obligé de prendre en main une clé ou un média utilisateur. Au simple contact du composant, le système reconnaît si la personne porte sur elle un média utilisateur autorisé. Pour cela, il suffit que le média utilisateur soit porté à une distance d'environ 5 à 10 cm du corps, par exemple dans la poche du pantalon, la poche de la veste ou dans un sac à main.

Restrictions :

- TouchGo ne peut pas être utilisé avec la fonction wireless.

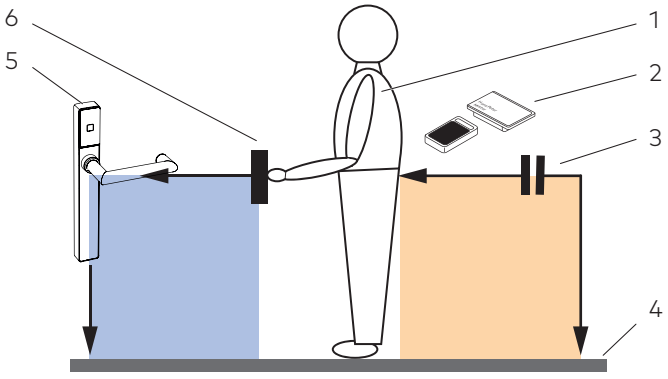
Documents complémentaires

- Directive de planification dormakaba c-lever pro TouchGo avec S-Module
- Manuel d'utilisation de dormakaba c-lever pro TouchGo

3.10.1 Fonctionnement RCID

RCID : Resistive Capacitive Identification

Lors d'un contact avec le composant (6 à 5), le système identifie si un média RCID (2) est porté près du corps et l'autorisation est évaluée.



1 Personne
2 Médias RCID
3 Transmission de signal capacitive (orange)
4 Masse commune (sol)
5 Composant TouchGo
6 Transmission du signal résistive via la poignée (bleu)

3.10.2 Aspects de sécurité

La technologie RCID se distingue des solutions traditionnelles par le fait qu'elle transfère les informations au moyen du champ électrostatique du corps [▶ 3.10.1], sans affecter le confort ni la sécurité. Par ailleurs, les fonctions sûres et flexibles des systèmes de fermeture électroniques sont préservées. Voir le chapitre Sécurité avec autorisations CardLink LEGIC [▶ 5.2] et le chapitre Sécurité avec l'autorisation Whitelist LEGIC [▶ 5.3].

La sécurité de l'ensemble du système est garantie à tout moment avec TouchGo, car les médias utilisateur perdus peuvent être effacés rapidement et facilement. Ceci permet de prévenir à la fois les failles de sécurité et les remplacements coûteux d'installations de fermeture complètes.

3.10.3 TouchGo E110

TouchGo E110 peut être utilisé avec les médias associés pour un maximum de 100 utilisateurs. Il dispose de la fonction TouchGo Mode office. TouchGo E110 ne nécessite aucun appareil de programmation ou logiciel système.

TouchGo E110 est autonome et ne peut pas être utilisé dans un sous-système evolo.

La programmation du TouchGo E110 est décrite dans le manuel d'utilisation de la c-lever pro TouchGo.

3.10.4 TouchGo E310

Les composants du TouchGo E310 s'intègrent facilement dans le logiciel système sélectionné, sans pour autant devoir renoncer à la sécurité. Le TouchGo E310 est une option confort n'affectant pas un dispositif de sécurité.

Le sous-système evolo utilise la technologie RFID éprouvée pour une identification et une gestion univoque. Pour ce faire, les données RFID dans le composant sont « mariées » (pairing) avec les données de la technologie TouchGo lors de la lecture. Cela signifie que l'autorisation d'accès attribuée est transférée à TouchGo et que le composant la reconnaît lors d'un contact tactile.

Les modifications futures dans l'autorisation, transférées via le Programmer (autorisation Whitelist) ou la technologie RFID (autorisation CardLink), sont également automatiquement transférées à TouchGo. En cas de perte ou de défaillance du média combiné ou uniquement du partenaire de pairing, l'autorisation peut être immédiatement supprimée. Dans d'autres cas, les composants individuels peuvent continuer à être utilisés, car un nouveau « mariage » peut être effectué directement sur les composants à tout moment.

TouchGo ne peut pas être utilisé avec la fonction wireless.

3.10.4.1 Autorisation Whitelist avec TouchGo

Pour les installations de fermeture avec autorisation Whitelist, le confort supplémentaire de TouchGo peut être utilisé pour les composants TouchGo. Tout comme le média RFID, le média combiné TouchGo RFID/RCID est simplement programmé dans le composant à l'aide de médias de programmation RFID ou bien placé sur le lecteur de table et les données de la technologie RFID sont enregistrées dans le logiciel système. L'autorisation d'accès de la technologie RFID est répartie sur les composants avec le Programmer. Le média combiné est présenté au composant autonome et « marié » (pairing) avec la technologie TouchGo lors de la lecture des données RFID. La même autorisation d'accès est transférée à TouchGo et le composant reconnaît l'autorisation via un contact tactile.

Les modifications ultérieures apportées à l'autorisation sont également automatiquement reprises dans TouchGo.

3.10.4.2 Autorisation CardLink avec TouchGo

Pour les installations de fermeture avec autorisations CardLink, le confort supplémentaire de TouchGo peut également être utilisé pour les composants TouchGo. L'attribution de l'autorisation s'effectue dans le logiciel système et est transférée aux composants autonomes via la technologie RFID.

En même temps que la transmission s'effectue, TouchGo est « marié » (pairing). Cela signifie que l'autorisation d'accès attribuée est transférée à TouchGo et que le composant la reconnaît via un contact tactile.

Les modifications ultérieures apportées à l'autorisation et le renouvellement de la validation seront transférés aux composants autonomes via la technologie RFID et le « mariage » (pairing) sera vérifié simultanément.

3.11 Sélection de vestiaire libre avec les serrures d'armoire 21 10 et 21 20

Cette option est uniquement disponible avec les modèles de serrure d'armoire 21 10 et 21 20.

En mode d'accès CardLink ou Whitelist, l'autorisation pour un vestiaire est attribuée à l'utilisateur de la même manière que pour un composant normal. En mode d'accès « Sélection de vestiaire libre avec CardLink » ou « Sélection de vestiaire libre avec Whitelist », les utilisateurs peuvent eux-mêmes occuper un vestiaire libre pour lequel ils sont autorisés. Un mode d'accès doit être configuré. Le nombre de vestiaires pouvant être occupés par chaque utilisateur est déterminé sur le média utilisateur à l'aide de l'assistant de serrure d'armoire. Un à quatre vestiaires peuvent être occupés. Un vestiaire occupé ne peut être ouvert qu'avec le média utilisateur correspondant ou avec un média de service. La sélection de l'utilisateur est alors supprimée et le vestiaire est à nouveau libre.

Les occupations de vestiaires peuvent être supprimées à l'aide des outils de gestion de votre système hôte, par exemple avec l'assistant de serrure d'armoire de dormakaba evolo Manager (KEM).

3.12 Boîte aux lettres/ascenseur

Un utilisateur ne peut utiliser son média utilisateur que pour ouvrir les boîtes aux lettres ou accéder en ascenseur aux étages pour lesquels il est autorisé.

Boîte aux lettres/ascenseur ne peut être configuré(e) que via le logiciel système.
Mobile Access est disponible à partir de la version du micrologiciel 42.38.
Wireless n'est pas possible.

Une unité comprend un gestionnaire de porte 91 15 et jusqu'à 6 modules 90 30 avec respectivement 8 sorties commutées. Le nombre de modules dépend du nombre de sorties nécessaires. 49 sorties au maximum peuvent ainsi être configurées.

Rapport des sorties aux composants requis :

Nombre de sorties	Nombre de composants
1	91 15 (gestionnaire de porte avec 1 sortie relais)
jusqu'à 9	91 15 + 1 x 90 30 (module d'extension avec 8 sorties relais)
jusqu'à 17	91 15 + 2 x 90 30
jusqu'à 25	91 15 + 3 x 90 30
jusqu'à 33	91 15 + 4 x 90 30
jusqu'à 41	91 15 + 5 x 90 30
jusqu'à 49	91 15 + 6 x 90 30

4 Variantes de système

Le sous-système evolo peut être utilisé dans différentes variantes système et reste extensible dans toutes les variantes.

Les exemples sélectionnés sont réalisables avec des médias LEGIC et MIFARE, même si les illustrations montrent principalement LEGIC. La différence réside dans les cartes de sécurité utilisées. Avec LEGIC, on utilise les cartes de sécurité C1 et C2, avec MIFARE la carte de sécurité C.

4.1 Programmation Whitelist

4.1.1 Autorisation Whitelist sans chaîne d'outils

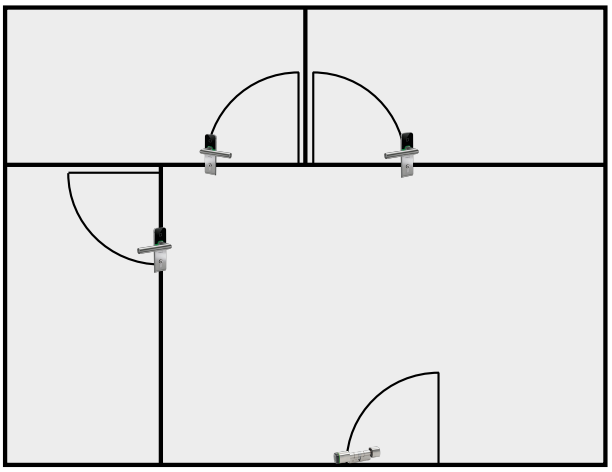
Pour les installations de fermeture de petite taille, les médias utilisateurs sont programmés directement dans les composants avec un Master. Aucun logiciel système ou programmer n'est nécessaire pour cette méthode. Wireless et Mobile Access sont également impossibles.

La programmation est décrite au chapitre Programmation avec des médias.

Master A, Master B et médias utilisateurs



Exemple d'installation :

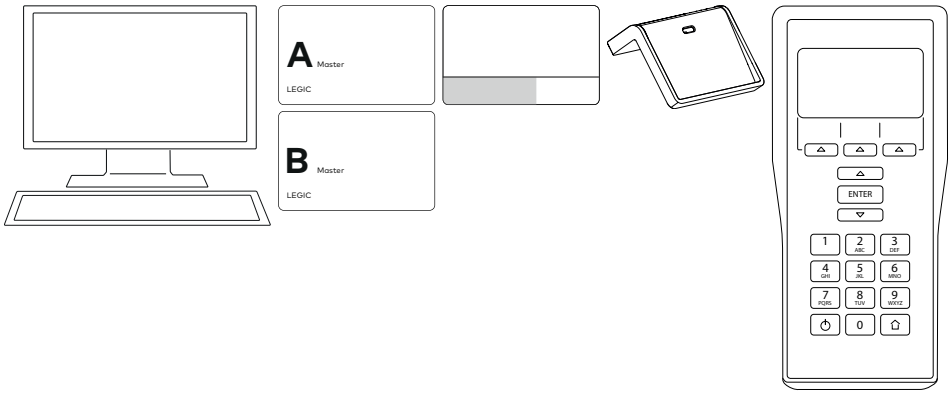


4.1.2 Autorisation Whitelist avec chaîne d'outils

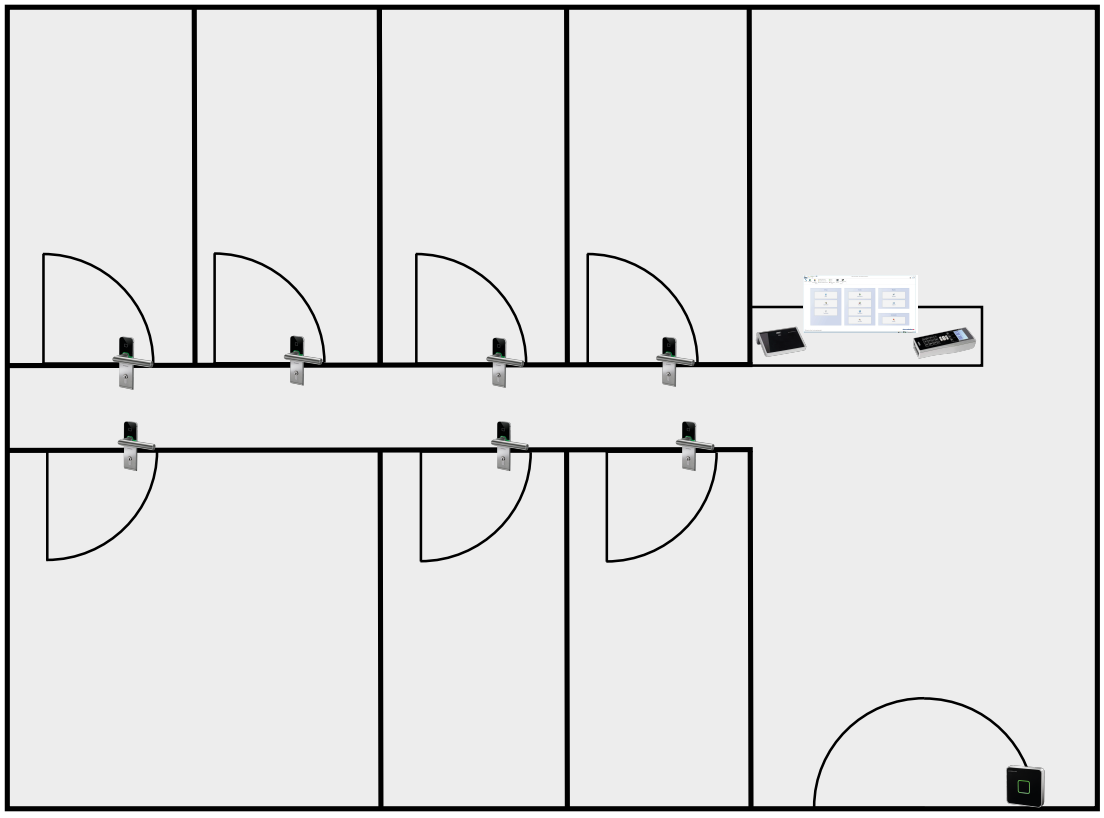
Pour les installations de fermeture plus importantes avec gestion du temps, les médias utilisateurs sont gérés avec le logiciel système. Les données d'autorisation sont transférées du logiciel aux composants avec le Programmer ou actualisées via wireless. Dans l'exemple sans wireless.

La programmation est décrite au chapitre Programmation avec le logiciel système et le Programmer [▶ 7.5.2].

Chaîne d'outils : Logiciel système avec Master, médias utilisateurs, lecteur de table et Programmer



Exemple d'installation :



4.2 Programmation CardLink

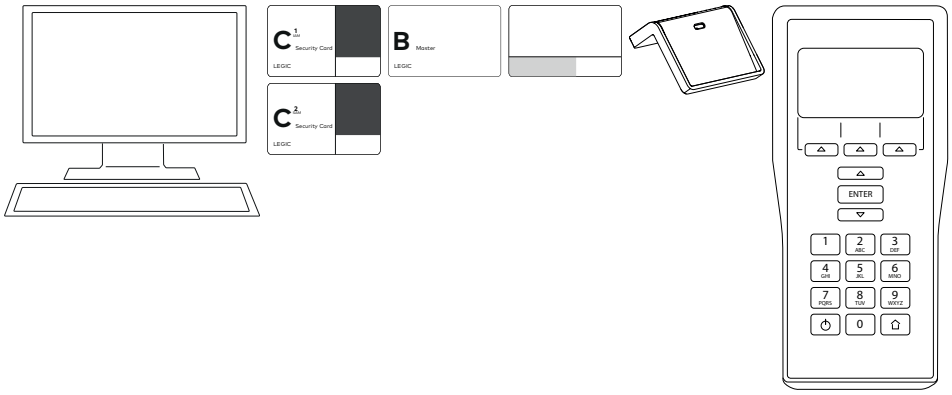
CardLink est programmé à l'aide du logiciel système.

La programmation est décrite au chapitre Programmation avec le logiciel système.

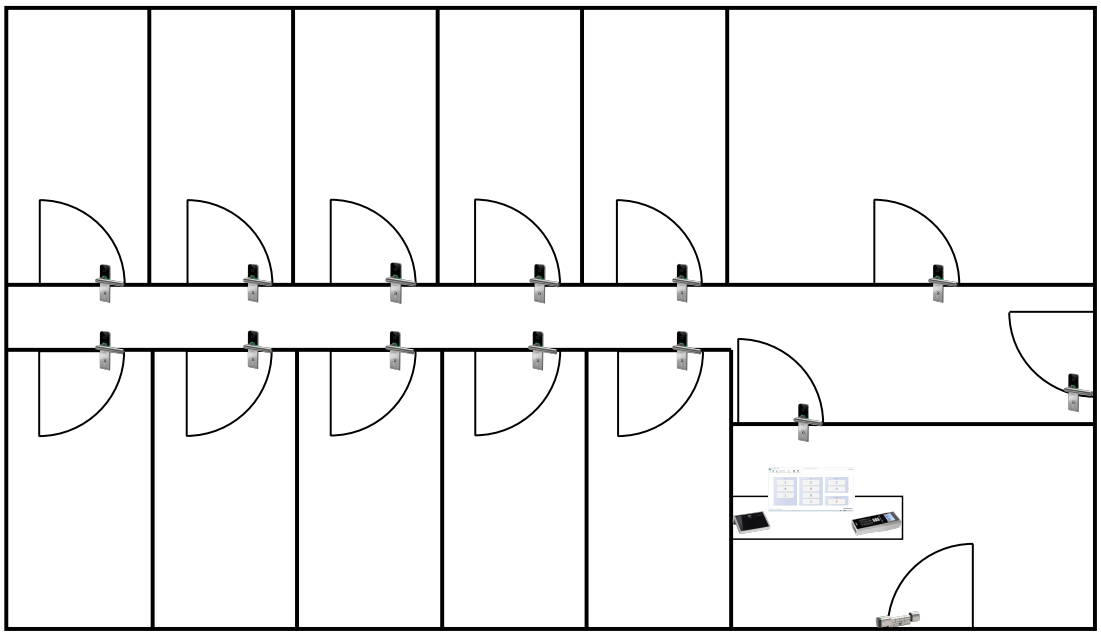
4.2.1 Autorisation CardLink via lecteur de table

Avec les installations de fermeture CardLink, les médias utilisateurs sont organisés avec le logiciel système. Les autorisations sont inscrites sur les médias utilisateurs avec le lecteur de table. Les composants nécessitent une initialisation seulement pour CardLink. Les nouvelles autorisations sont transférées du logiciel système avec le lecteur de table dans les médias utilisateurs. Dans ce cas, les validations sont prises en charge par les différents composants autonomes qui sont configurés à cet effet. La fonction wireless est également prise en charge.

Chaîne d'outils : Logiciel système avec carte de sécurité, Master, médias utilisateurs, lecteur de table et Programmer



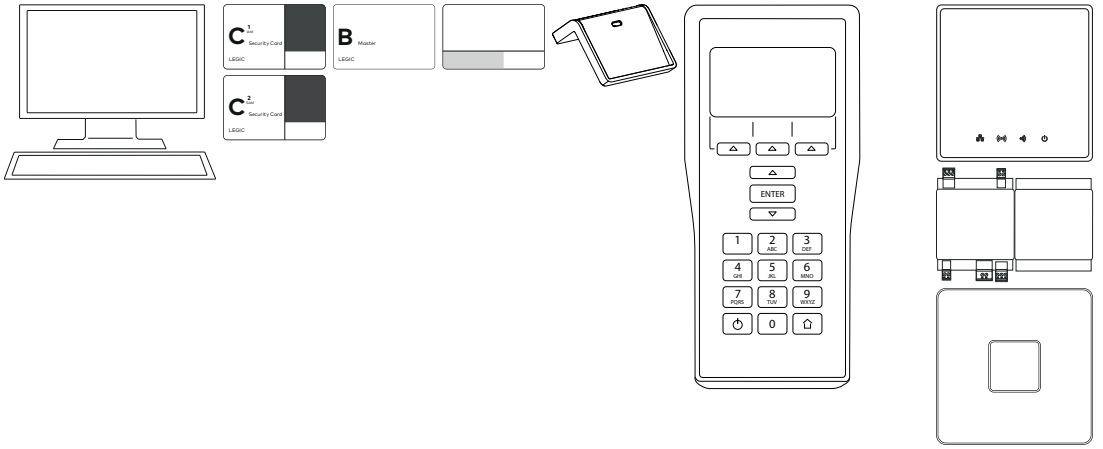
Exemple d'installation :

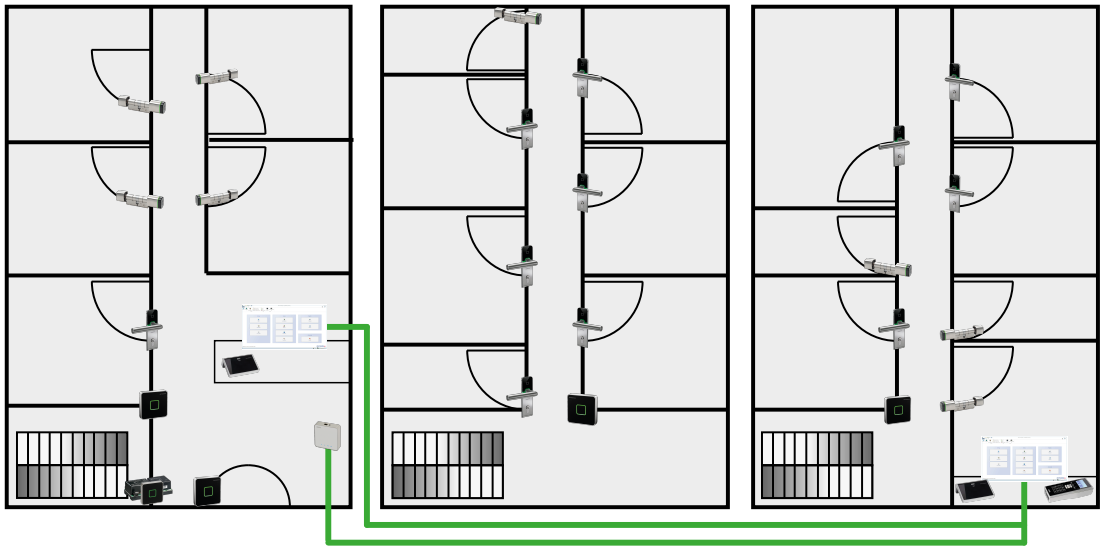


4.2.2 Autorisation CardLink via lecteur de mise à jour

Un lecteur de mise à jour CardLink est utilisé à la place du terminal pour attribuer de nouvelles autorisations d'accès dans les médias utilisateurs. Le lecteur est connecté au logiciel système via un hub de communication*. De nouvelles autorisations d'accès pour les utilisateurs peuvent ainsi être accordées ou retirées en ligne à tout moment. Dans ce cas, les validations sont effectuées par le lecteur de mise à jour.

Chaîne d'outils : Logiciel système avec carte de sécurité, Master, médias utilisateurs, lecteur de table, Programmer, passerelle réseau et lecteur de mise à jour 91 15 avec module d'extension 90 43.





Transférer les autorisations CardLink sans hub de communication vers Update Reader

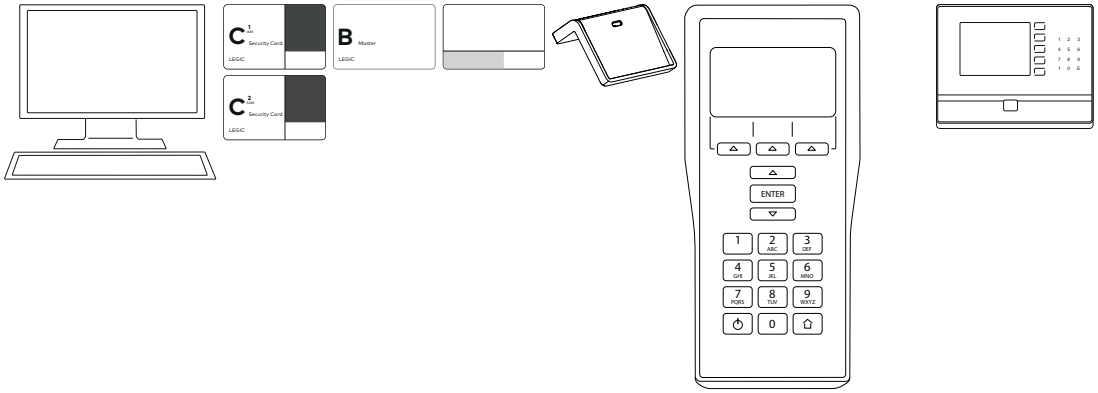
Les autorisations CardLink peuvent être transférées au lecteur de mise à jour à l'aide du Programmer 1460.

Le confort que peuvent offrir les autorisations d'accès accordées en ligne et indépendamment du temps est ainsi supprimé.

4.2.3 Autorisation CardLink via terminal

Ce type d'autorisation CardLink est particulièrement adapté aux installations de fermeture avec modification fréquente des habilitations pour utilisateur. Pour attribuer de nouvelles autorisations d'accès dans les médias utilisateurs, le terminal connecté au logiciel système est utilisé. De nouvelles autorisations d'accès pour les utilisateurs peuvent ainsi être accordées ou retirées à tout moment. Dans ce cas, les validations sont effectuées par le terminal.

Chaîne d'outils : Logiciel système avec carte de sécurité, Master, médias utilisateurs, lecteur de table, Programmer et terminal



Exemple d'installation :



4.3 Vue d'ensemble des variantes de micrologiciels

Fonction/Micrologiciel	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	jusqu'à 200	jusqu'à 200	jusqu'à 200	jusqu'à 200	jusqu'à 200	jusqu'à 200	jusqu'à 200	jusqu'à 200
Autorisations Whitelist								
Entrées Whitelist (UID/Card ID) – mode hors ligne	4000	1000	1000[5]	4000	4000 (mode hors ligne)	4000	4000 (mode hors ligne)	4000 (mode hors ligne) jusqu'à 30 000 (utilisation en ligne avec le hub de communication 90 40-K7)
Entrées Whitelist (UID/Card ID) – mode en ligne avec Wireless Gateway 90 40-K7				jusqu'à 30 000	jusqu'à 30 000		jusqu'à 30 000	jusqu'à 30 000
Autorisations en fonction du temps	✓	✓	✓	✓	✓	✓	✓	✓
Désactiver la programmation manuelle	✓	✓	✓	✓	✓	✓	✓	✓
Autorisations CardLink								
Validation	✓	—	✓	✓	✓	✓	✓	✓
Droit individuel Porte[4]	jusqu'à 60	—	jusqu'à 60	jusqu'à 60	jusqu'à 60	jusqu'à 60	jusqu'à 60	jusqu'à 60
Droit individuel Groupe de portes[4]	jusqu'à 39	—	jusqu'à 39	jusqu'à 39	jusqu'à 39	jusqu'à 39	jusqu'à 39	jusqu'à 39
Réservation Droit individuel Porte[4]	jusqu'à 18	—	jusqu'à 18	jusqu'à 18	jusqu'à 18	jusqu'à 18	jusqu'à 18	jusqu'à 18
Réservation Droit individuel Groupe de portes[4]	jusqu'à 11	—	jusqu'à 11	jusqu'à 11	jusqu'à 11	jusqu'à 11	jusqu'à 11	jusqu'à 11
Droit de groupes de portes	512	—	512	512	512	512	512	512
Entrées Blacklist	400	—	400	400	400	400	400	400
Médias de service	✓	—	✓	✓	✓	✓	✓	✓
Traceback des médias[3]	60	—	60	60	60	60	60	60
Médias TouchGo	—	—	1000	—	—	—	—	—
Fonctions avancées								
Wireless	—	—	—	✓	✓	—	✓	✓

Fonction/Micrologiciel	E300[A]	E305[B]	E310[C]	E320[D]	E321[E]	E340[F]	E360[G]	E361[H]
Mémoire Traceback de composants	2000	2000	2000	2000	2000	2000	2000	2000
Mode Pass[1]	Option	—	Option	Option	Option	Option	Option	Option
Profils de temps	15 et « Toujours »	15 et « Toujours »	15 et « Toujours »	15 et « Toujours »	15 et « Toujours »	15 et « Toujours »	15 et « Toujours »	15 et « Toujours »
Plage horaire pour chaque profil de temps	12	12	12	12	12	12	12	12
Périodes de vacances	20	20	20	20	20	20	20	20
Jours particuliers A+B	32+32	32+32	32+32	32+32	32+32	32+32	32+32	32+32
Fonctions TimePro	✓	✓	✓	✓	✓	✓	✓	✓
S-Module[2]	Option	—	Option	Option	Option	Option	Option	Option
Master T et média de service	✓	✓	✓	✓	✓	✓	✓	✓
Mobile Access								
NFC/HCE	✓	—	—	✓	✓	✓	✓	✓
Bluetooth	—	—	—	—	—	✓	✓	✓

Légende :

1 Uniquement pour c-lever pro.

2 Standard pour les lecteurs, en option pour c-lever pro.

3 Uniquement avec médias MIFARE DESFire et LEGIC advant.
En fonction de la taille du segment/fichier
Valeur par défaut selon la spécification des médias. Peut être plus grande ou plus petite.

4 Selon les types d'autorisation utilisés.

5 RCID et RFID.

A E300 – evolo V4

B E305 – Boîte aux lettres/ascenseur
E345 – Boîte aux lettres/ascenseur avec Mobile Access

C E310 – TouchGo

D E320 – Wireless

E E321 – Wireless avec surveillance de porte
Des composants supplémentaires, tels que des contacts de cadre de porte et des capteurs de serrure (pêne demi-tour, pêne dormant), sont nécessaires.

F E340 – Mobile Access

G E360 – Wireless et Mobile Access

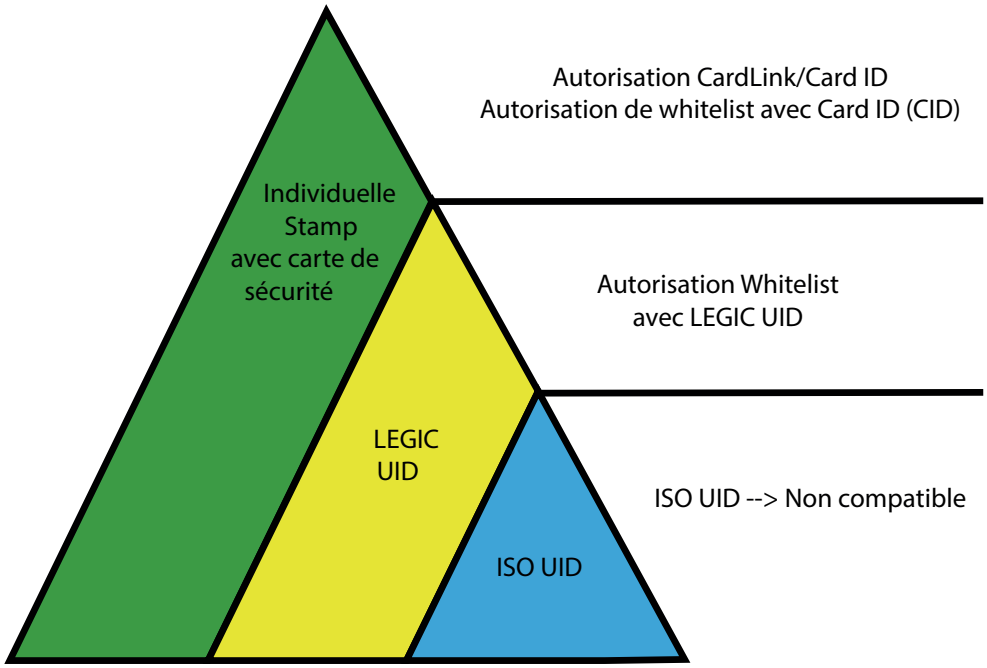
H E361 – Wireless avec surveillance de porte et Mobile Access
Des composants supplémentaires, tels que des contacts de cadre de porte et des capteurs de serrure (pêne demi-tour, pêne dormant), sont nécessaires.

5 Fonctions de sécurité

Ce chapitre décrit les fonctions de sécurité possibles pour LEGIC et MIFARE dans les installations de fermeture, qui peuvent être sélectionnées en fonction des exigences de sécurité souhaitées.

5.1 Les degrés de sécurité LEGIC

Les degrés de sécurité suivants sont disponibles pour les types d'autorisation.



Marquage individuel
Un marquage individuel est défini pour chaque installation de fermeture. Ce marquage sert à l'identification des médias LEGIC spécifiques à l'installation. Le marquage est défini par la carte de sécurité C1 ou C2 dans l'installation de fermeture respective.

UID LEGIC
L'UID LEGIC est utilisé pour les installations de fermeture normales avec Whitelist. Avec l'UID LEGIC, le numéro unique (UID) est également vérifié sur les médias via une fonction LEGIC.

Indication : le logiciel système KEM utilise uniquement l'UID LEGIC.

5.2 Sécurité avec autorisations CardLink LEGIC

Marquage individuel
Un marquage individuel est nécessaire pour l'utilisation d'une autorisation CardLink avec LEGIC.

Chaque composant électronique, ainsi que le lecteur de table, dispose de matériel LEGIC qui fonctionne avec ce marquage. La carte de sécurité C1 et/ou C2 est nécessaire pour que le marquage spécifique à l'installation puisse être intégré dans l'installation de fermeture. Avec cette carte de sécurité, le marquage est transféré sur le composant correspondant. Une nouvelle carte de sécurité est requise pour chaque installation de fermeture. En cas d'utilisation d'un marquage, le logiciel système KEM, le lecteur de table et les composants correspondants doivent être initialisés avec celui-ci. La carte de sécurité doit ensuite être conservée dans un endroit sûr (p. ex. un coffre-fort).

5.3 Sécurité avec l'autorisation Whitelist LEGIC

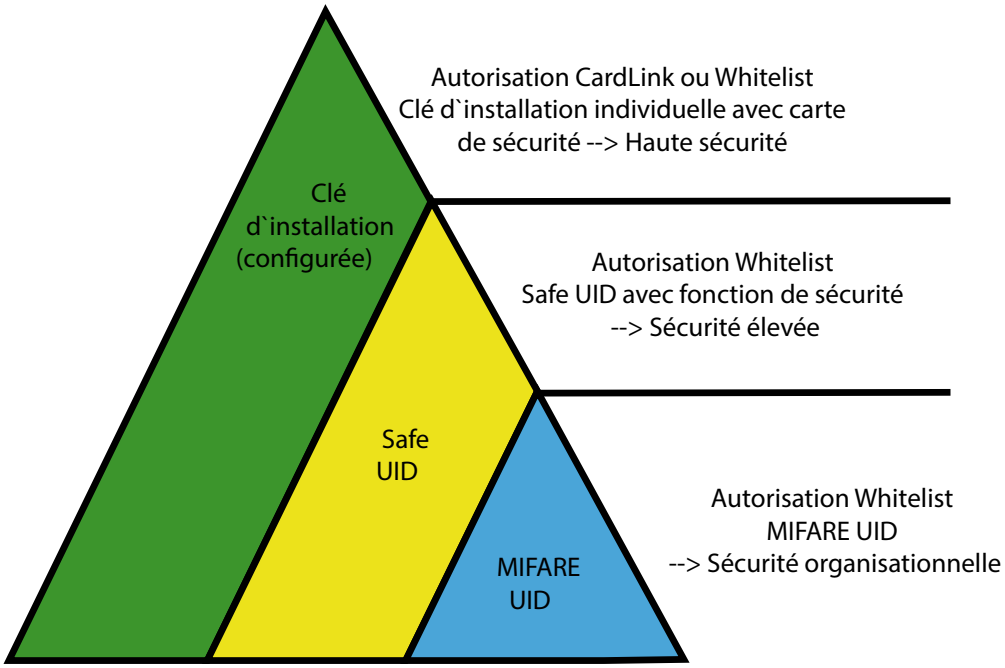
Card ID (CID)
À la place de l'UID, un CID individuel est attribué aux médias par le système.

Ce CID est inscrit dans la mémoire du média avec un marquage LEGIC individuel. Ce marquage est défini par la carte de sécurité C1. Chaque installation nécessite une propre carte de sécurité pour assurer la sécurité. Si le marquage LEGIC individuel est utilisé, le logiciel système KEM et le lecteur de table doivent être initialisés avec celui-ci. La carte de sécurité doit être ensuite conservée dans un endroit sûr (p. ex. un coffre-fort).

UID LEGIC
Avec l'UID LEGIC, la fonction LEGIC est utilisée pour sécuriser l'UID (numéro unique) des médias utilisateurs. La sécurité d'un UID s'en trouve ainsi considérablement améliorée car la fonction LEGIC vérifie l'UID.

5.4 Les degrés de sécurité MIFARE

Les degrés de sécurité suivants sont disponibles pour les types d'autorisation.



Clé de l'installation (Sitekey)
La clé d'installation est adaptée à une utilisation dans des installations de fermeture avec des exigences de sécurité élevées.

La clé d'installation est une clé spécifique attribuée individuellement à chaque installation de fermeture. Cette clé est générée automatiquement par une puce de sécurité. Cette puce de sécurité supplémentaire est intégrée à chaque composant et règle, après initialisation, le cryptage et le décryptage individuels de toutes les données écrites par le système sur les médias utilisateurs.

Safe UID
Ce degré de sécurité est utilisé pour les installations de fermeture normales.

Avec Safe UID, le numéro unique (UID) est en outre enregistré sous forme cryptée sur la mémoire médias. L'UID est seulement reconnu comme valide si les données de médias utilisateurs correspondent.

MIFARE UID
Ce degré de sécurité convient avant tout aux applications organisationnelles.

Les médias MIFARE sont conformes à la norme ISO 14443A. Celle-ci définit que le numéro unique (UID) peut être lu sans autre clé. Pour ce degré de sécurité, seul l'UID du transpondeur est utilisé pour l'identification.

5.5 Sécurité avec autorisations CardLink MIFARE

Clé d'installation
Une clé d'installation (Sitekey) est nécessaire pour l'utilisation d'une autorisation CardLink ou d'un Master T.

Chaque composant électronique, ainsi que le lecteur de table, dispose de matériel de sécurité spécial qui travaille avec cette clé d'installation. La carte de sécurité C est nécessaire pour que la clé spécifique à l'installation puisse être intégrée à l'installation de fermeture. Cette carte de sécurité permet de transmettre la clé d'installation à l'installation de fermeture correspondante. Une carte de sécurité individuelle est nécessaire pour chaque installation de fermeture.

Si une clé d'installation est utilisée, le logiciel système, le lecteur de table et les médias de programmation correspondants doivent être initialisés avec celle-ci. La carte de sécurité doit être ensuite conservée dans un endroit sûr (p. ex. un coffre-fort).

5.6 Sécurité avec l'autorisation Whitelist MIFARE

Card ID (CID)
À la place de l'UID, un CID individuel est attribué aux médias par le système. Ce CID est crypté avec une clé d'installation individuelle, puis inscrit dans la mémoire des médias. Cette clé d'installation est définie par une carte de sécurité C.

La carte de sécurité C peut être obtenue via le canal de distribution. Cette carte de sécurité permet d'initialiser les composants électroniques avec la clé individuelle de l'installation. Une carte de sécurité individuelle est nécessaire pour chaque installation.

Si une clé d'installation est utilisée, le logiciel système, le lecteur de table et les médias de programmation correspondants doivent être initialisés avec celle-ci. La carte de sécurité doit être ensuite conservée dans un endroit sûr (p. ex. un coffre-fort).

Safe UID
Le niveau de sécurité Safe UID est adapté aux applications avec des exigences de sécurité élevées.

L'application Kaba KCA dans les médias utilisateurs est une condition préalable pour l'utilisation de la fonction Safe UID. Avec le Safe UID, l'UID (numéro unique) des médias est en plus vérifié par une application spéciale dans les mémoires des médias. La sécurité d'une UID est ainsi considérablement améliorée, car le contenu de l'application n'est pas librement accessible et crypté.

MIFARE UID (selon ISO 14443A)
L'UID (numéro unique) permet de programmer une autorisation dans la Whitelist.

Lorsque l'UID est conforme à la norme ISO 14443A, il peut alors être inscrit dans la Whitelist. Conformément à la norme ISO, cet UID peut être librement lu et n'est pas autrement sécurisé. L'utilisation de ce niveau de sécurité n'est recommandée que pour des applications organisationnelles avec de faibles exigences de sécurité.

5.7 Master T

Le Master T est une forme spéciale de média master pour les composants autonomes. Les Master T utilisés dans une installation de fermeture sont uniquement valides pour une période donnée et ont des fonctions limitées. Ceci assure une grande flexibilité dans la gestion des installations de fermeture, car un Master T peut être remis au personnel de service sans qu'il soit nécessaire de lui remettre le Master A ou B, essentiel pour la sécurité.



Un Master T peut uniquement être utilisé si les composants ont été préalablement configurés avec un Master B et le Programmer 1460.

Master T pour LEGIC :
Le logiciel système permet de définir des médias Master T pour LEGIC. Un Master T est dérivé de la carte de sécurité et ne peut être utilisé que comme Master T.

Master T pour MIFARE :
Le logiciel système permet de définir des médias Master T pour MIFARE. Un Master T peut être dérivé de la carte de sécurité C.

Les médias Master T pour LEGIC et MIFARE possèdent les propriétés suivantes :

- Utilisation dans les deux types d'autorisation : CardLink et Whitelist.
- Actualisation des composants (les composants doivent être configurés).
- Réglage de l'horloge des composants.
- Lecture du Traceback.
- Durée de validité limitée dans le temps.

6 Composants

Les composants evolo offrent une grande variété de fonctions, qui sont résumées dans l'aperçu suivant. Des composants avec une protection mécanique renforcée sont disponibles pour les zones essentielles à la sécurité. Les informations détaillées figurent dans les manuels d'utilisation séparés et dans le catalogue produits.

6.1 Espaces de mémoire

Les espaces de mémoire suivants sont disponibles pour la mémoire réinscriptible des médias utilisateurs :

	MIFARE		LEGIC
Autorisations	**classic**	**DESFire**	**advant**
	en octets	en octets	en octets
Taille de mémoire des médias utilisateurs	1 k	8 k	4 k
Médias utilisateurs CTC	—		3 k
Taille de mémoire des applications standard	288	744	848
Kaba Common Application (KCA) Safe UID	48	32	—
CardLink (192 octets de données utiles)	216	192	216
Nombre maximal d'autorisations sur un média utilisateur :			
Maximum de 512 groupes de portes configurés :	– jusqu'à 39 droits individuels – jusqu'à 11 réservations		
Sans groupes de portes :	– jusqu'à 60 droits individuels – jusqu'à 18 réservations		
Entrées de statut :			
État des composants (32 octets de données utiles)	48	32	56
Identification (32 octets de données utiles)	48	32	64
Traceback (60 entrées)	—	488	512

6.2 Données techniques

Médias utilisateurs
Cartes

Désignation	**Valeurs**
Couleurs (mise en page d'impression)	• dormakaba (rouge ou bleu) • votre design personnalisé
Conditions ambiantes	
Indice de protection	IP66 Résiste à l'humidité, mais pas à l'immersion dans l'eau. Une utilisation comme clé de piscine, par exemple, n'est pas recommandée.
Température	-25 ... +70 °C
Humidité de l'air	0 ... 95 % HR, sans condensation
Capacité de mémoire des médias	

K-BE-MID	8 ko (MIFARE DESFire EV3)
K-BE-MIC	1 ko (MIFARE classic)
K-BE-ADT	4 ko/3,5 ko (LEGIC advant/MIFARE DESFire EV3)
K-BE-CTC	1 ko/3 ko (LEGIC prime/advant)



Les cartes sont protégées contre le piratage et le clonage.

Porte-clés

Désignation	**Valeurs**
Couleurs	Bleu, noir, rouge, blanc
Conditions ambiantes	
Indice de protection	IP65
Température	-20 ... +55 °C
Humidité de l'air	0 ... 95 % HR, sans condensation
Capacité de mémoire des médias	
A-BE-MID	8 ko (MIFARE DESFire EV3)
A-BE-ADT	4 ko/3,5 ko (LEGIC advant/MIFARE DESFire EV3)
A-BE-CTC	1 ko/3 ko (LEGIC prime/advant)

Clé avec clip

Désignation	**Valeurs**
Clip	
Couleurs	
Inserts de couleur du clip	Noir, argenté, violet, jaune, vert, rouge, bleu
Conditions ambiantes	
Indice de protection	IP67 Résiste à une immersion temporaire dans l'eau.
Température	-20 ... +70 °C
Humidité de l'air	0 ... 95 % HR, sans condensation
Capacité de mémoire des médias	
S-BE-MID	8 ko (MIFARE DESFire EV3)
S-BE-MIC	1 ko (MIFARE classic EV1)
S-BE-ADT	4 ko/3,5 ko (LEGIC advant/MIFARE DESFire EV3)
S-BE-CTC	1 ko/3 ko (LEGIC prime/advant)
Clé	
Systèmes de fermeture mécaniques	
dormakaba eco	
dormakaba expert	
dormakaba gemini	
dormakaba matrix	
dormakaba penta	
dormakaba quattro	
dormakaba pextra	
dormakaba AP2000	

Kaba star
Kaba star cross
Kaba 20

Médias utilisateurs TouchGo
Porte-clés

Désignation	**Valeurs**
Couleurs	
Médias utilisateurs	Noir, blanc
Dimensions	
l x H x P	36 x 60 x 12 mm
Alimentation électrique	
Pile	3 V CR2450 lithium
Conditions ambiantes	
Indice de protection	IP 53
Température	-25 ... +65 °C
Humidité de l'air	0 ... 95 % HR, sans condensation
Capacité de mémoire des médias	
A-BE-TGO	
A-BE-TGO-MID	8 ko (MIFARE DESFire EV3)
A-BE-TGO-MID-ADT	4 ko/3,5 ko (LEGIC advant/MIFARE DESFire EV3)
A-BE-TGO-MID-CTC	1 ko/3 ko (LEGIC prime/advant)

Bracelet

Désignation	**Valeurs**
Couleurs	Gris
Dimensions	
l x H x P	56 x 53 x 17 mm
Alimentation électrique	
Pile	3 V CR2450 lithium
Conditions ambiantes	
Indice de protection	IP67 (étanche)
Température	-25 ... +65 °C
Humidité de l'air	0 ... 95 % HR, sans condensation
Capacité de mémoire des médias	
B-BE-TGO	8 ko (MIFARE DESFire EV3)
B-BE-TGO-MID	1 ko (LEGIC prime)
B-BE-TGO-ADT	4 ko/3,5 ko (LEGIC advant/MIFARE DESFire EV3)
B-BE-TGO-CTC	1 ko/3 ko (LEGIC prime/advant)

Porte-carte

Désignation	**Valeurs**
Couleurs	
Porte-carte	Noir, argenté-noir
Dimensions	

l x H x P	90 x 58 x 14 mm
Alimentation électrique	
Pile	3 V CR2430 lithium
Conditions ambiantes	
Indice de protection	IP 53
Température	-25 ... +65 °C
Humidité de l'air	0 ... 95 % HR, sans condensation
Capacité de mémoire des médias	
H-BE-TGO	selon le média introduit.

6.3 Médias master

Les composants peuvent être programmés dans le mode de programmation avec 2 types différents de médias master, Master A et Master B (). Ces médias sont exclusivement utilisés pour la répartition de l'autorisation et ne possèdent eux-mêmes aucune autorisation d'accès.

Médias master	MIFARE	LEGIC	Fonctions
Master A 	✓	✓	– Master d'une installation avec structure master A/B – Les composants sont remis en mode programmation avec Master B – Programmer les composants avec Master B
Master B 	✓	✓	– Master d'une installation – Les composants sont remis en mode programmation – Programmer les composants avec des médias utilisateurs
Master T 	✓	✓	– Master T pour l'actualisation de composants – Valide uniquement pendant une période déterminée – Fonctions restreintes
Master B RCID 			RCID Uniquement TouchGo E110 – Master d'une installation – Les composants sont remis en mode programmation – Programmer les composants avec des médias utilisateurs

6.4 Cartes de sécurité

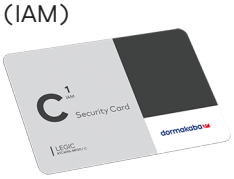
Les cartes de sécurité sont utilisées dans un environnement LEGIC ou MIFARE. Les fonctions des cartes de sécurité se différencient en fonction de la technologie utilisée.

Il existe différentes cartes de sécurité pour LEGIC :

- Carte de sécurité C1 pour la segmentation des médias spécifiques à l'installation
- Carte de sécurité C2 pour l'initialisation de l'installation avec lecteur de table et composants de validation dans CardLink

Pour MIFARE, il y a la carte de sécurité C :

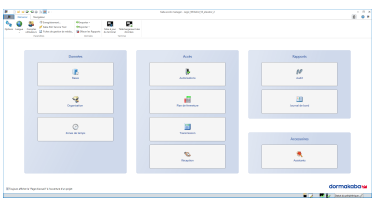
La carte de sécurité C est nécessaire pour que la clé spécifique à l'installation dans un environnement MIFARE puisse être intégrée à l'installation de fermeture. Celle-ci définit la clé d'installation ainsi que l'organisation de la mémoire des médias utilisateurs.

Cartes de sécurité	MIFARE	LEGIC	Fonctions
Carte de sécurité C 	✓	—	– Définition de la clé de l'installation (Sitekey) – Configurer des médias – Initialiser le système – Écrire les applications sur des cartes vierges.
Carte de sécurité C1 (IAM) 	—	✓	– Définition du marquage – Initialiser le système – Configurer des médias – Créer des segments
Carte de sécurité C2 (SAM) 	—	✓	– Définition du marquage – Initialiser le système – Autorisation d'écriture pour lecteur de table et composant de validation – Écrire sur les segments

Autorisation d'écriture avec la carte de sécurité C2
Avec la carte de sécurité C2, les composants qui doivent écrire des données sur les segments des médias utilisateurs doivent recevoir une autorisation d'écriture. Il s'agit par exemple de lecteurs de table ou de composants de validation. Pour une description de l'application, voir le chapitreMessages lors de l'utilisation de la carte de sécurité C2 [▶ 8.5].

6.5 Chaîne d'outils

Une chaîne d'outils comprend les outils de programmation utilisés dans le sous-système. Ces outils disposent de diverses fonctions pour la configuration, la gestion, la lecture et l'écriture de composants et de médias.

Outil	Fonctions
Programmer 1460 	• Configuration des propriétés des composants. • Programmation des composants. • Lecture du Traceback des composants. • Mises à jour du micrologiciel sur les composants. • Mise en service de composants wireless.
Logiciel système : par exemple dormakaba evolo Manager (KEM). 	• Gestion d'autorisations. • Gestion de médias et de personnes. • Gestion d'installations de fermeture. • Évaluation de données Traceback.

Outil	Fonctions
Lecteur de table 91 08 	• Lecture et écriture de médias. • Organisation de la mémoire de médias.
Wireless Gateway 90 40-K7 	• Configuration des propriétés des composants. • Programmation des composants. • Lecture du Traceback des composants. • Mises à jour du micrologiciel sur les composants.
Wireless Extender 90 41 	• Extension de la portée radio du hub de communication. • Pour composants wireless.
Extension wireless sur le lecteur distant 	91 15 + 90 43 • Connexion wireless pour lecteurs distants. • Mise à jour CardLink via wireless.
Mobile Access 	Mobile Access • Gestion/accès via smartphone avec Bluetooth ou NFC.

7 Programmer / configurer les composants

Avant la programmation, la technologie de média doit être définie. Voir le chapitre Définir la technologie de média [▶ 7.1].

Les droits d'accès et autres droits sont ensuite attribués par la programmation / configuration des composants.

- Les composants wireless nécessitent une mise en service wireless avant leur première utilisation.
  Voir la documentation wireless

7.1 Définir la technologie de média

Les composants Multi RFID (MRD) sont configurés lors de la première utilisation avec un Master LEGIC ou MIFARE sur la technologie utilisée par les composants. Les composants se comportent ensuite comme défini pour les types d'autorisation LEGIC (LEA) ou MIFARE (MID).

Marche à suivre

- Tenir le média master environ 1 s devant l'unité de saisie.
  - La technologie de média du média master (Legic ou MIFARE) a été transmise au périphérique.

Indication : Après une réinitialisation INI, la technologie doit être à nouveau définie.

7.2 Méthodes de programmation et configuration

Méthodes :

- Sans système hôte avec médias master et utilisateurs,
  voir le chapitre Programmer avec des médias [▶ 7.4]
- Avec logiciel système et programmeur,
  voir le chapitre Programmation avec logiciel système et programmeur [▶ 7.5.2]
- Produits TouchGo :
  voir le chapitre Programmer des produits TouchGo
- Applications Wireless :
  Mise en service avec logiciel système et programmeur,
  puis configuration via le hub de communication,
  voir manuel et description du système du Programmer et du hub de communication
- Appareils Mobile Access : Après la transmission de la configuration avec le programmeur : Initialiser l'appareil pour Mobile Access,
  voir le chapitre Initialisation de l'appareil pour Mobile Access [▶ 7.6.2].
- evolo smart :
  L'application guide l'utilisateur tout au long du processus.

7.3 Programmer des produits TouchGo

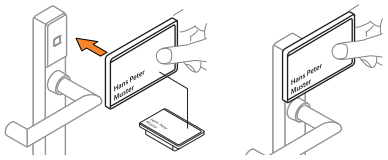
Avec TouchGo, l'autorisation d'accès est contrôlée lors du contact avec les composants.

Produit	
c-lever pro TouchGo E110	seulement RCID ; autonome Whitelist Voir le manuel d'utilisation du dormakaba c-lever pro TouchGo
c-lever pro TouchGo E310	RFID et RCID ; sous-système evolo Voir chapitre Programmer TouchGo E310.

7.3.1 Programmer TouchGo E310

Avec le TouchGo E310, des médias RFID sont utilisés pour la programmation. Pour que la fonction TouchGo prenne effet, un appariement (Pairing) des médias utilisateurs RFID et RCID doit avoir lieu après la programmation.

Utiliser les médias master et les médias utilisateurs du TouchGo E310 comme suit :



Maintenir les médias master RFID et les médias combinés (médias utilisateurs RCID/RFID) contre l'unité de saisie RFID (signal lumineux) du TouchGo E310.

7.3.1.1 Programmation manuelle de la Whitelist

7.3.1.1.1 Programmer les médias utilisateurs

Après présentation du Master B, le composant obtient le droit temporaire suivant :

- Accorder l'autorisation d'accès au média utilisateur présenté (enregistré dans la White-list).

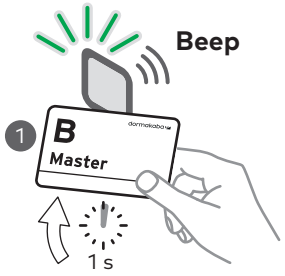
Si le Master B est maintenu à nouveau ou après 20 s sans qu'un média soit présenté devant le composant, le droit temporaire est à nouveau retiré du composant.

Conditions préalables

- Structure A/B ou
- structure B présente

Marche à suivre :

1. Maintenir le Master B env. **1 s** devant l'unité de saisie.



⇨ Le voyant vert s'allume.

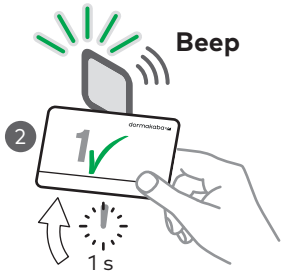
⇨ 1 signal court retentit.

⇨ Le voyant vert s'éteint.

Si aucun média n'est maintenu devant l'unité de saisie pendant 20 s, le processus est automatiquement interrompu :

-> Les modifications ont été appliquées et 1 signal long retentit.

2. Maintenir le média utilisateur env. **1 s** devant l'unité de saisie.



⇨ Le voyant vert s'allume.

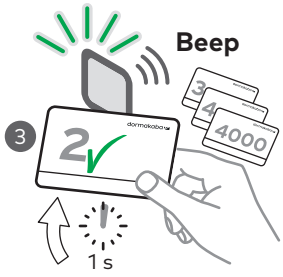
⇨ 1 signal court retentit.

⇨ Le voyant vert s'éteint.

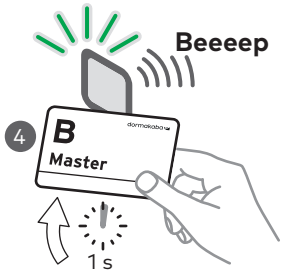
⇨ Le média utilisateur a été inscrit dans la Whitelist.

⇨ Le média utilisateur a accès au composant.

Programmer d'autres médias utilisateurs : Répéter l'étape 2.



3. Maintenir le Master B env. 1 s devant l'unité de saisie.



⇨ Le voyant vert s'allume.

⇨ 1 signal long retentit.

⇨ Le voyant vert s'éteint.

⇨ Les modifications ont été appliquées.

⇨ La programmation est terminée.

Si nécessaire, accorder des autorisations d'accès avec d'autres Master B.

7.3.1.1.2 Annuler une autorisation individuelle

Annuler l'autorisation d'accès d'un média utilisateur.

Après présentation du Master B, le composant obtient le droit temporaire suivant :

- Retirer l'autorisation d'accès au média utilisateur présenté (la supprimer de la Whitelist).

Si le Master B est présenté à nouveau, le droit temporaire est à nouveau retiré du composant.

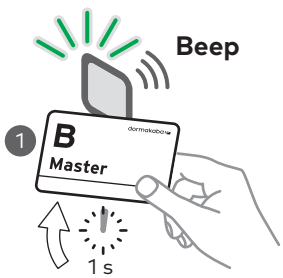
Conditions préalables

- Média utilisateur avec autorisation d'accès.
- Structure A/B ou
- structure B présente

Marche à suivre

Présenter des médias utilisateurs supplémentaires, si nécessaire.

1. Maintenir le Master B env. **1 s** devant l'unité de saisie.



⇨ Le voyant vert s'allume.

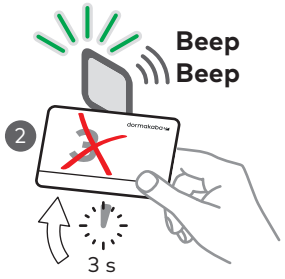
⇨ 1 signal court retentit.

⇨ Le voyant vert s'éteint.

Si aucun média n'est maintenu devant l'unité de saisie pendant 20 s, le processus est automatiquement interrompu :

-> Les modifications ont été appliquées et 1 signal long retentit.

2. Maintenir le média utilisateur env. **3 s** devant l'unité de saisie.



⇨ Le voyant vert s'allume.

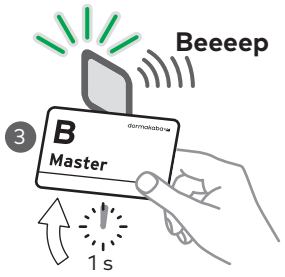
⇨ 2 signaux courts retentissent.

⇨ Le voyant vert s'éteint.

⇨ Le média utilisateur a été retiré de la Whitelist. Le média utilisateur n'a pas accès au composant.

Présenter des médias utilisateurs supplémentaires, si nécessaire.

3. Maintenir le Master B env. 1 s devant l'unité de saisie.



⇨ Le voyant vert s'allume.

⇨ 1 signal long retentit.

⇨ Le voyant vert s'éteint.

⇨ Les modifications ont été appliquées.

⇨ Le processus est terminé.

7.3.1.1.3 Annuler toutes les autorisations d'accès

Après présentation du Master B, le composant obtient le droit temporaire suivant :

- Annuler toutes les autorisations d'accès accordées par le Master B (les supprimer de la Whitelist).

Remarque : Le Master B conserve le droit d'accorder des autorisations d'accès.

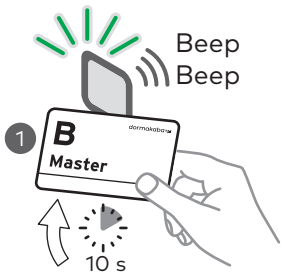
Marche à suivre

AVIS

Perte de données

Si le Master B est maintenu enfoncé pendant **15 s**, une réinitialisation INI est effectuée. La réinitialisation INI efface tous les réglages et données stockés dans le composant.

1. Tenir le Master B environ **10 s**devant l'unité de saisie.



   ⇨ Le voyant vert s'allume.

   ⇨ À partir de la version du micrologiciel 42 : 1 signal long et 2 signaux courts retentissent.
   Avant la version du micrologiciel 42 : 2 signaux courts retentissent.

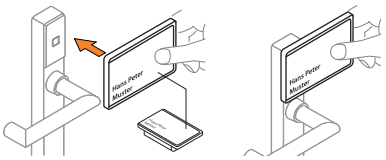
   ⇨ Le voyant vert s'éteint.

   ⇨ Tous les droits d'accès attribués par le Master B ont été annulés.

⇨ Le processus est terminé.

7.3.1.2 Appariement RCID/RFID

Le TouchGo E310 est utilisé dans le système dormakaba evolo. La technologie RFID est utilisée pour la programmation et l'identification. Pour que la fonction TouchGo prenne effet, un appariement des médias utilisateurs RFID et RCID est nécessaire.



7.3.1.2.1 Accorder une autorisation RCID

Autorisation Whitelist
L'autorisation est programmée avec le média master RFID et les médias combinés (médias utilisateurs RCID/RFID) directement via l'unité de saisie RFID. Lors de la lecture du média combiné, les données RFID sont « mariées » (Pairing) avec les données RCID (TouchGo).

Autorisation CardLink
L'autorisation est configurée via le logiciel système et appliquée avec les médias combinés (médias utilisateurs RFID/RCID) directement via l'unité de saisie RFID. Lors de la lecture du média combiné, les données RFID sont « mariées » (Pairing) avec les données RCID (TouchGo).

Les modifications ultérieures de l'autorisation et la mise à jour de la validation sont transférées aux composants via la technologie RFID et l'appariement est vérifié simultanément.

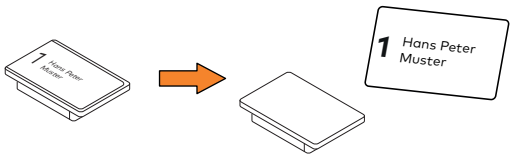
Les médias RCID ne peuvent pas être programmés deux fois (appariement déjà existant).

7.3.1.2.2 Annuler l'autorisation RCID

Annuler l'autorisation RCID en séparant le couple RCID/RFID. Ceci est impossible avec les médias combinés.

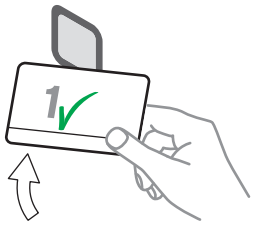
Marche à suivre

1. Séparer physiquement le média RFID et le média RCID.
   Retirer la carte du porte-carte, par exemple.



2. Placer le média RCID à env. 2 m sur une autre table.
   ⇨ Ne pas porter le média RCID sur vous.

3. Présenter le média RFID devant le composant.



⇨ L'appariement a été annulé.

7.3.1.3 Paramétrer TouchGo E310 dans le logiciel système

Dans les installations de fermeture gérées par un logiciel système, des composants TouchGo E310 peuvent également être utilisés. Les médias combinés (médias utilisateurs RCID/RFID) sont programmés dans les composants avec un média master RFID ou les données RFID sont enregistrées et gérées avec le lecteur de table. Les autorisations d'accès du média combiné sont ensuite transférées aux composants avec le Programmateur (autorisation Whitelist) ou les données RFID du média combiné (autorisation CardLink).

7.3.1.4 Fonction TimePro

7.3.1.4.1 Mode bureau avec Whitelist

1 média avec TimePro :

Le fonctionnement est identique à l'opération du Mode bureau.
La fonction TimePro permet une activation temporisée.

Plusieurs entrées TimePro :

Activation via le média combiné ou la fonction TouchGo (toucher la poignée intérieure).
Désactivation via le média combiné ou la plage horaire réglée.

7.3.1.4.2 Mode bureau avec CardLink

Activation de la fonction TimePro ou du Mode bureau via le média combiné ou via TouchGo (toucher la poignée intérieure).
Désactiver via le média combiné ou la plage horaire réglée.

7.3.1.5 Programmer les autorisations Mode bureau

La fonction TouchGo Mode bureau est décrite au chapitre Opération.
Ce chapitre décrit comment accorder ou annuler l'autorisation d'activer ou de désactiver le Mode bureau.

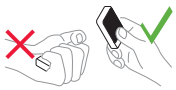
E310
Les autorisations sont attribuées aux utilisateurs à l'aide du logiciel système.

E110
Programmation sur le TouchGo E110 :

- Accorder l'autorisation : Chapitre [▸ 7.3.1.5.1]
- Annuler l'autorisation :
  - Autorisation individuelle : Chapitre [▸ 7.3.1.5.2]
  - Toutes les autorisations : Chapitre [▸ 7.3.1.5.3]

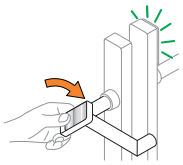
7.3.1.5.1 Accorder l'autorisation Mode bureau

- Ne pas enserrer le média master et le média utilisateur avec la main.



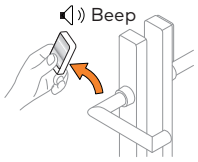
- Ne tenir que 1 seul média en main. S'assurer que les autres médias sont à au moins 2 m de distance.

1. Tenir le média master en main.
2. Toucher la poignée intérieure avec l'index.



⇨ Le voyant vert s'allume.

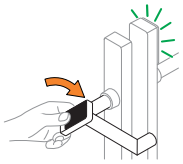
3. Retirer l'index/le média master.



⇨ Le voyant vert s'éteint.

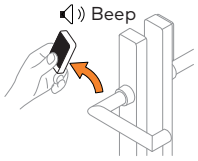
⇨ 1 signal court retentit.

4. Tenir le média utilisateur en main.
5. Toucher la poignée intérieure avec l'index.



⇨ Le voyant vert s'allume.

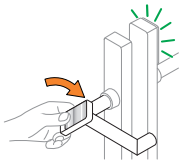
6. Retirer l'index/le média utilisateur.



⇨ Le voyant vert s'éteint.

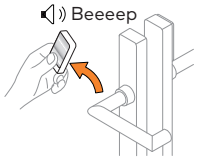
⇨ 1 signal court retentit.

7. Tenir le média master en main.
8. Toucher la poignée intérieure avec l'index.



⇨ Le voyant vert s'allume.

9. Retirer l'index/le média master.



⇨ Le voyant vert s'éteint.

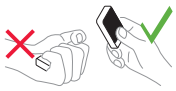
⇨ 1 signal long retentit.

⇨ L'autorisation d'accès en Mode bureau a été accordée.

7.3.1.5.2 Annuler une autorisation Mode bureau individuelle

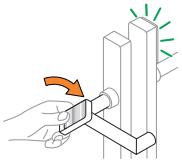
Annuler l'autorisation Mode bureau d'un média utilisateur.

- Ne pas enserrer le média master et le média utilisateur avec la main.



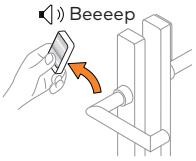
- Ne tenir que 1 seul média en main. S'assurer que les autres médias sont à au moins 2 m de distance.

1. Tenir le média master en main.
2. Toucher la poignée intérieure avec l'index.



⇨ Le voyant vert s'allume.

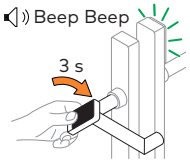
3. Retirer l'index/le média.



⇨ Le voyant vert s'éteint.

⇨ 1 signal long retentit.

4. Tenir le média utilisateur en main.
5. Toucher la poignée intérieure avec l'index pendant 3 s.

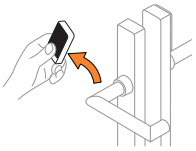


⇨ Le voyant vert s'allume.

⇨ 2 signaux courts retentissent.

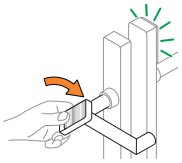
⇨ L'autorisation Mode bureau du média est annulée.

6. Retirer l'index/le média utilisateur.



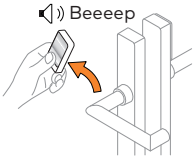
⇨ Le voyant vert s'éteint.

7. Tenir le média master en main.
8. Toucher la poignée intérieure avec l'index.



⇨ Le voyant vert s'allume.

9. Retirer l'index/le média master.



⇨ Le voyant vert s'éteint.

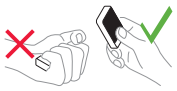
⇨ 1 signal long retentit.

⇨ L'autorisation Mode bureau est annulée.

7.3.1.5.3 Annuler toutes les autorisations Mode bureau

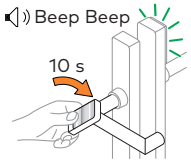
Annuler toutes les autorisations Mode bureau enregistrées dans les composants.

- Ne pas enserrer le média master et le média utilisateur avec la main.



- Ne tenir que 1 seul média en main. S'assurer que les autres médias sont à au moins 2 m de distance.

1. Tenir le média master en main.
2. Toucher la poignée intérieure pendant 10 s.

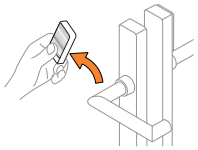


⇨ Le voyant vert s'allume.

⇨ 2 signaux courts retentissent.

⇨ Toutes les autorisations sont annulées.

3. Retirer l'index/le média master.



⇨ Le voyant vert s'éteint.

⇨ Toutes les autorisations du Mode bureau sont annulées.

7.3.2 Médias utilisateurs perdus/défectueux

L'annulation des autorisations pour les médias utilisateurs perdus ou défectueux est nécessaire pour la sécurité des installations. Les autorisations des médias utilisateurs restants sont ensuite reprogrammées.

Séquence :

1. Annuler toutes les autorisations. Voir [▸ 7.3.1.1.3]
   ⇨ Les autorisations d'accès sont annulées.
   ⇨ Les autorisations Mode bureau sont annulées.
2. Reprogrammer les médias utilisateurs.
   ⇨ Reprogrammer les autorisations d'accès. Voir [▸ 7.3.1.1.1]
   ⇨ Reprogrammer les autorisations Mode bureau. Voir [▸ 7.3.1.5]

7.4 Programmer avec des médias

Présenter un média master (env. 1 s) active le mode programmation.
Quitter le mode programmation :
Automatiquement, 20 secondes après la dernière présentation du média (time-out) ou en présentant à nouveau le média master (env. 1 s).

7.4.1 Cartes

7.4.1.1 Définir le média master supérieur

- Le média master supérieur est le média supérieur d'un composant.
- 1 média master supérieur doit être attribué à chaque composant.
- 1 seul média master supérieur peut être attribué à chaque composant.
- Le premier média master présenté à un composant est enregistré comme média master supérieur.

Structure A/B

- Dans une structure A/B, le média master supérieur doit être un Master A.
- Un Master A peut accorder des droits Master B à des médias. Voir le chapitre « Créer une structure A/B ».
- Un Master A peut retirer des droits à des médias Master B. Voir chapitre « Effacer Master B du composant ».
- Une réinitialisation INI peut être lancée sur le composant avec un Master A, voir chapitre « Réinitialisation INI avec des médias master ».

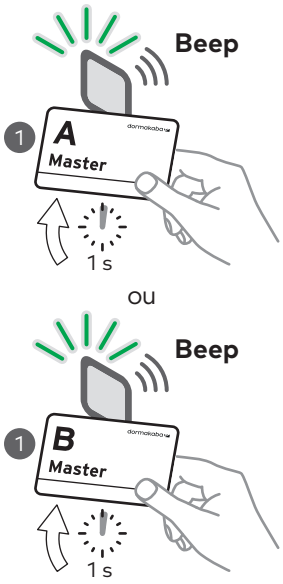
Structure B

- Dans une structure B, le média master supérieur doit être un Master B.
- Une réinitialisation INI peut être lancée sur le composant avec un Master-B, voir chapitre « Réinitialisation INI avec des médias master ».

Conditions préalables

- Le composant est dans l'état de livraison d'usine, voir Réinitialisation INI.

Marche à suivre

	Maintenir le média master (A ou B) pendant env. **1 s** devant l'unité de saisie. -> Le voyant vert s'allume. -> 1 signal court retentit. -> Le vert s'éteint. -> Le média master présenté a été enregistré comme média master supérieur.	1x court

7.4.1.2 Créer une structure A/B

Après présentation du Master A, le composant obtient le droit temporaire suivant :

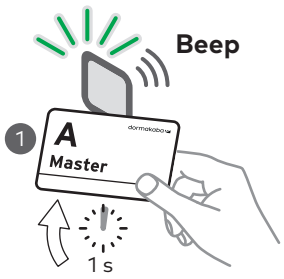
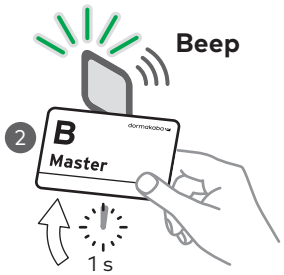
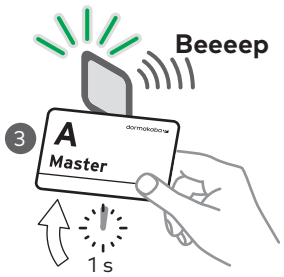
- Accorder aux Master B présentés le droit d'attribuer des droits d'accès aux médias utilisateurs.

Si le Master A est présenté à nouveau, le droit temporaire est à nouveau retiré du composant.

Conditions préalables

- Le Master A présenté est le média supérieur du composant.
  Voir chapitre « Définir le média master supérieur »

Marche à suivre

	Maintenir le Master A env. **1 s** devant l'unité de saisie. -> Le voyant vert s'allume. -> 1 signal court retentit. -> Le vert s'éteint.	1x court
	Si aucun média n'est maintenu devant l'unité de saisie pendant 20 s, le processus est automatiquement interrompu : -> Les modifications ont été appliquées et 1 signal long retentit.	
	Maintenir le Master B env. **1 s** devant l'unité de saisie. -> Le voyant vert s'allume. -> 1 signal court retentit. -> Le vert s'éteint. -> Le Master B a le droit d'attribuer des droits d'accès aux médias utilisateurs. -> La structure A/B est créée.	1x court
	Présenter d'autres Master B si nécessaire.	
	Maintenir le Master A env. **1 s** devant l'unité de saisie. -> Le voyant vert s'allume. -> 1 signal long retentit. -> Le vert s'éteint.	1x long

7.4.1.3 Accorder des autorisations d'accès

Après présentation du Master B, le composant obtient le droit temporaire suivant :

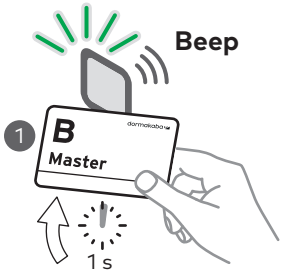
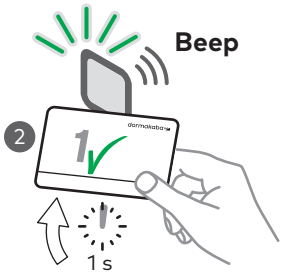
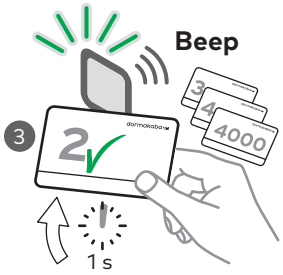
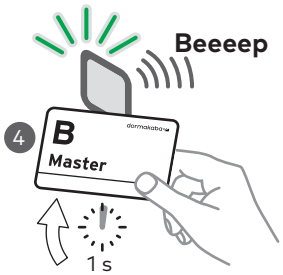
- Accorder l'autorisation d'accès au média utilisateur présenté (enregistré dans la White-list).

Si le Master B est présenté à nouveau, le droit temporaire est à nouveau retiré du composant.

Conditions préalables

- Structure A/B ou
- structure B présente

Marche à suivre

	Maintenir le Master B env. **1 s** devant l'unité de saisie. -> Le voyant vert s'allume. -> 1 signal court retentit. -> Le vert s'éteint.	1x court
	Si aucun média n'est maintenu devant l'unité de saisie pendant 20 s, le processus est automatiquement interrompu : -> Les modifications ont été appliquées et 1 signal long retentit.	
	Maintenir le média utilisateur env. **1 s** devant l'unité de saisie. -> Le voyant vert s'allume. -> 1 signal court retentit. -> Le vert s'éteint. -> Le média utilisateur a été inscrit dans la Whitelist. Le média utilisateur a accès au composant.	1x court
	Si nécessaire, ajouter d'autres médias utilisateurs à la Whitelist : Répéter l'étape 2.	1x court
	Maintenir le Master B env. 1 s devant l'unité de saisie. -> Le voyant vert s'allume. -> 1 signal long retentit. -> Le vert s'éteint. -> Les modifications ont été appliquées.	1x long
	Si nécessaire, accorder des autorisations d'accès avec d'autres Master B.	

7.4.1.4 Annuler des autorisations d'accès individuelles

Après présentation du Master B, le composant obtient le droit temporaire suivant :

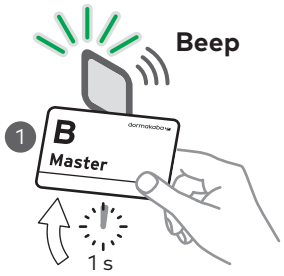
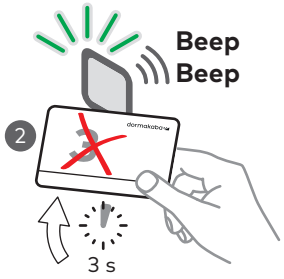
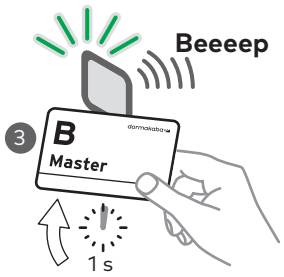
- Retirer l'autorisation d'accès au média utilisateur présenté (la supprimer de la Whitelist).

Si le Master B est présenté à nouveau, le droit temporaire est à nouveau retiré du composant.

Conditions préalables

- Média utilisateur avec autorisation d'accès.
- Structure A/B ou
- structure B présente

Marche à suivre

	Maintenir le Master B env. **1 s** devant l'unité de saisie. -> Le voyant vert s'allume. -> 1 signal court retentit. -> Le vert s'éteint.	1x court
	Si aucun média n'est maintenu devant l'unité de saisie pendant 20 s, le processus est automatiquement interrompu : -> Les modifications ont été appliquées et 1 signal long retentit.	
	Maintenir le média utilisateur env. **3 s** devant l'unité de saisie. -> Le voyant vert s'allume. -> 2 signaux courts retentissent. -> Le vert s'éteint. -> Le média utilisateur a été retiré de la Whitelist. Le média utilisateur n'a pas accès au composant. Présenter des médias utilisateurs supplémentaires, si nécessaire.	2x court
	Maintenir le Master B env. 1 s devant l'unité de saisie. -> Le voyant vert s'allume. -> 1 signal long retentit. -> Le vert s'éteint. -> Les modifications ont été appliquées.	1x long

7.4.1.5 Effacer le Master B du composant

Après présentation du Master A, le composant obtient les droits temporaires suivants :

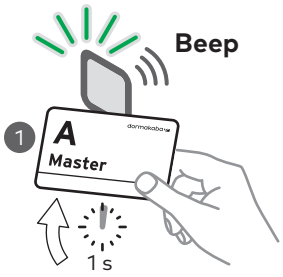
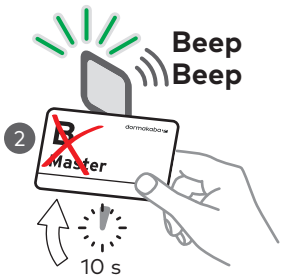
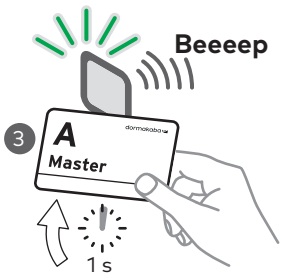
- Annuler toutes les autorisations d'accès accordées par le Master B présenté (les supprimer de la Whitelist).
- Retirer au Master B présenté le droit d'accorder des autorisations d'accès.

Si le Master A est présenté à nouveau, les droits temporaires sont à nouveau retirés du composant.

Conditions préalables

- Le Master B a obtenu ses droits du Master A
- Structure A/B présente

Marche à suivre

	Maintenir le Master A env. **1 s** devant l'unité de saisie. -> Le voyant vert s'allume. -> 1 signal court retentit. -> Le vert s'éteint.	1x court
	Si aucun média n'est maintenu devant l'unité de saisie pendant 20 s, le processus est automatiquement interrompu : -> Les modifications ont été appliquées et 1 signal long retentit.	
	Maintenir le Master B devant l'unité de saisie (env. 10 s) jusqu'à ce que 2 signaux courts retentissent. -> Le voyant s'allume en vert tant que le Master B est présenté. Présenter d'autres Master B si nécessaire.	2x court
	Maintenir le Master A env. **1 s** devant l'unité de saisie. -> Le voyant vert s'allume. -> 1 signal long retentit. -> Le vert s'éteint. -> Les modifications ont été appliquées.	1x long

7.4.1.6 Annuler toutes les autorisations d'accès attribuées par le Master B

Après présentation du Master B, le composant obtient le droit temporaire suivant :

- Annuler toutes les autorisations d'accès accordées par le Master B (les supprimer de la Whitelist).

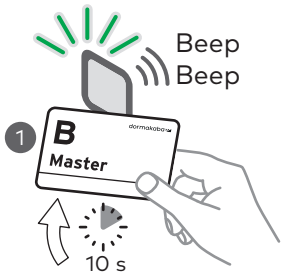
Remarque : Le Master B conserve le droit d'accorder des autorisations d'accès.

Marche à suivre

AVIS

Perte de données

Si le Master B est maintenu pendant **15 s**, une réinitialisation INI est effectuée.
La réinitialisation INI efface tous les réglages et données stockés dans le composant.

	Tenir le Master B environ **10 s**devant l'unité de saisie. -> Le voyant vert s'allume. -> 1 signal long et 1 signal court retentissent (à partir de la version 42 du micrologiciel). -> (Avant la version du micrologiciel 42 : 2 signaux courts retentissent.) -> Le vert s'éteint. -> Tous les droits d'accès attribués par le Master B ont été annulés.	À partir de la version du micrologiciel 42 : 1x long 1x court Avant la version du micrologiciel 42 : 2x court

7.4.2 Clé

7.4.2.1 Définir le média master supérieur

- Le média master supérieur est le média supérieur d'un composant.
- 1 média master supérieur doit être attribué à chaque composant.
- 1 seul média master supérieur peut être attribué à chaque composant.
- Le premier média master inséré dans le cylindre est enregistré comme média master supérieur.

Structure A/B

- Dans une structure A/B, le média master supérieur doit être un Master A.
- Un Master A peut accorder des droits Master B à des médias. Voir le chapitre « Créer une structure A/B ».
- Un Master A peut retirer des droits à des médias Master B. Voir chapitre « Effacer Master B du composant ».
- Une réinitialisation INI peut être lancée sur le composant avec un Master A, voir chapitre « Réinitialisation INI avec des médias master ».

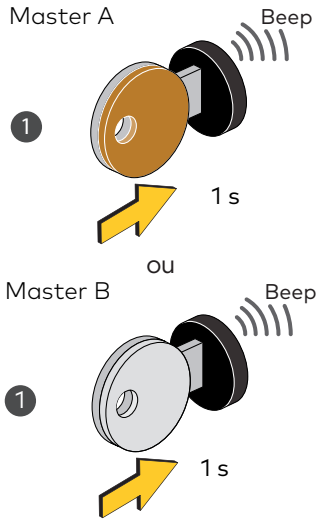
Structure B

- Dans une structure B, le média master supérieur doit être un Master B.
- Une réinitialisation INI peut être lancée sur le composant avec un Master B, voir chapitre « Réinitialisation INI avec des médias master ».

Conditions préalables

- Le composant est dans l'état de livraison d'usine, voir Réinitialisation INI.

Marche à suivre

	Insérer le média master (A ou B) dans le cylindre pendant env. **1 s**. -> 1 signal court retentit. -> Le média master présenté a été enregistré comme média master supérieur.	1x court

7.4.2.2 Créer une structure A/B

Après insertion du Master A, le composant obtient le droit temporaire suivant :

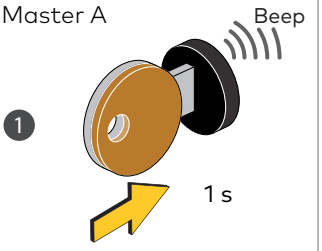
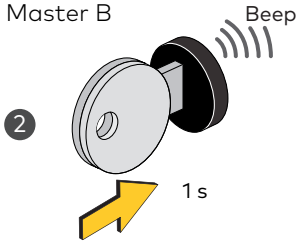
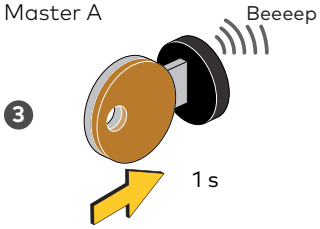
- Accorder au Master B inséré dans le cylindre le droit d'attribuer des droits d'accès aux médias utilisateurs.

Si le Master A est inséré à nouveau, le droit temporaire est à nouveau retiré du composant.

Conditions préalables

- Le Master A inséré dans le cylindre est le média supérieur du composant.
  Voir chapitre « Définir le média master supérieur »

Marche à suivre

Master A Beep  	Insérer le Master A dans le cylindre pendant env. **1 s**. -> 1 signal court retentit.	1x court
	Si aucun média n'est inséré dans le cylindre pendant 20 s, le processus est automatiquement terminé : -> Les modifications ont été appliquées et 1 signal long retentit.	
Master B Beep  	Insérer le Master B dans le cylindre pendant env. **1 s**. -> 1 signal court retentit. -> Le Master B a le droit d'attribuer des droits d'accès aux médias utilisateurs. -> La structure A/B est créée.	1x court
	Présenter d'autres Master B si nécessaire.	
Master A Beeeep  	Insérer le Master A dans le cylindre pendant env. **1 s**. -> 1 signal long retentit.	1x long

7.4.2.3 Accorder des autorisations d'accès

Après insertion du master B, le composant obtient le droit temporaire suivant :

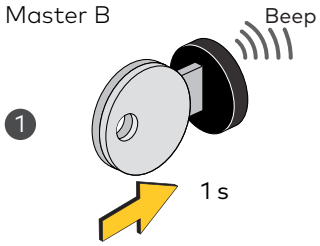
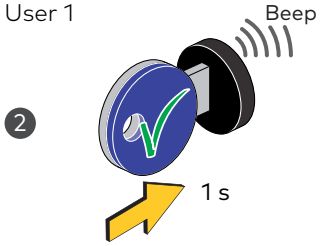
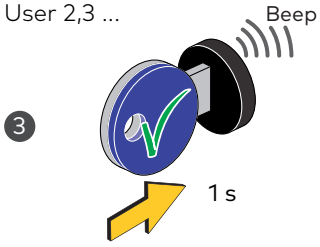
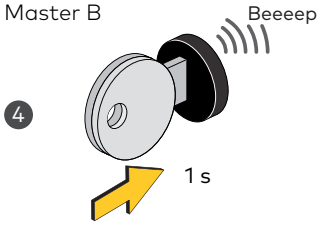
- Accorder l'autorisation d'accès au média utilisateur inséré dans le cylindre (enregistré dans la Whitelist).

Si le Master B est inséré à nouveau, le droit temporaire est à nouveau retiré du composant.

Conditions préalables

- Structure A/B ou
- structure B présente

Marche à suivre

Master B Beep  	Insérer le Master B dans le cylindre pendant env. **1 s**. -> 1 signal court retentit.	1x court
	Si aucun média n'est inséré dans le cylindre pendant 20 s, le processus est automatiquement terminé : -> Les modifications ont été appliquées et 1 signal long retentit.	
User 1 Beep  	Insérer le média utilisateur dans le cylindre pendant env.**1 s**. -> 1 signal court retentit. -> Le média utilisateur a été inscrit dans la Whitelist. Le média utilisateur a accès au composant.	1x court
User 2,3 ... Beep  	Si nécessaire, ajouter d'autres médias utilisateurs à la Whitelist : Répéter l'étape 2.	1x court
Master B Beeeep  	Insérer le Master B dans le cylindre pendant env. 1 s. -> 1 signal long retentit. -> Les modifications ont été appliquées.	1x long
	Si nécessaire, accorder des autorisations d'accès avec d'autres master B.	

7.4.2.4 Annuler des autorisations d'accès individuelles

Après insertion du master B, le composant obtient le droit temporaire suivant :

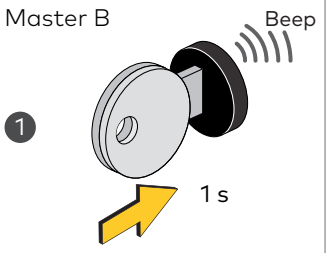
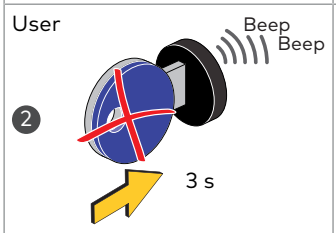
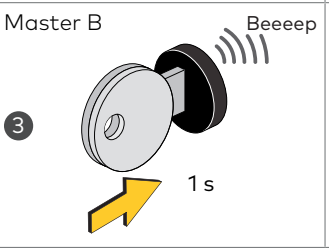
- Retirer l'autorisation d'accès au média utilisateur inséré dans le cylindre (la supprimer de la Whitelist).

Si le Master B est inséré à nouveau, le droit temporaire est à nouveau retiré du composant.

Conditions préalables

- Média utilisateur avec autorisation d'accès.
- Structure A/B ou
- structure B présente

Marche à suivre

Master B Beep  	Insérer le Master B dans le cylindre pendant env. **1 s**. -> 1 signal court retentit.	1x court
	Si aucun média n'est inséré dans le cylindre pendant 20 s, le processus est automatiquement terminé : -> Les modifications ont été appliquées et 1 signal long retentit.	
User Beep Beep  	Insérer le média utilisateur dans le cylindre pendant env.**3 s**. -> 2 signaux courts retentissent. -> Le média utilisateur a été retiré de la Whitelist. Le média utilisateur n'a pas accès au composant. Présenter des médias utilisateurs supplémentaires, si nécessaire.	2x court
Master B Beeeep  	Insérer le Master B dans le cylindre pendant env. 1 s. -> 1 signal long retentit. -> Les modifications ont été appliquées.	1x long

7.4.2.5 Effacer le Master B du composant

Après insertion du Master A, le composant obtient les droits temporaires suivants :

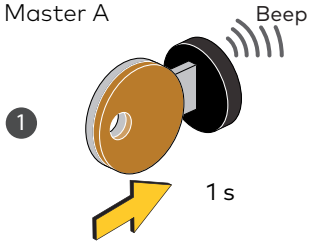
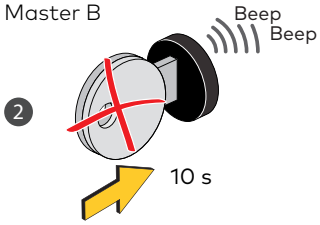
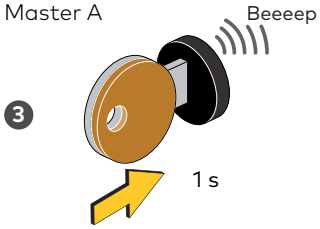
- Annuler toutes les autorisations d'accès accordées par le Master B inséré (les supprimer de la Whitelist).
- Retirer au Master B inséré le droit d'accorder des autorisations d'accès.

Si le Master A est inséré à nouveau, les droits temporaires sont à nouveau retirés du composant.

Conditions préalables

- Le Master B a obtenu ses droits du Master A
- Structure A/B présente

Marche à suivre

Master A Beep  	Insérer le Master A dans le cylindre pendant env. **1 s**. -> 1 signal court retentit.	1x court
	Si aucun média n'est inséré dans le cylindre pendant 20 s, le processus est automatiquement terminé : -> Les modifications ont été appliquées et 1 signal long retentit.	
Master B Beep Beep  	Insérer le Master B dans le cylindre (env. 10 s), jusqu'à ce que 2 signaux courts retentissent. Présenter d'autres Master B si nécessaire.	2x court
Master A Beeeep  	Insérer le Master A dans le cylindre pendant env. **1 s**. -> 1 signal long retentit. -> Les modifications ont été appliquées.	1x long

7.4.2.6 Annuler toutes les autorisations d'accès attribuées par le Master B

Après insertion du Master B, le composant obtient le droit temporaire suivant :

- Annuler toutes les autorisations d'accès accordées par le Master B (les supprimer de la Whitelist).

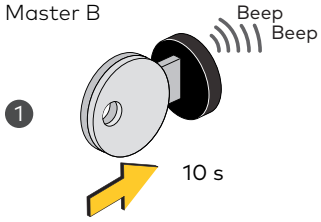
Remarque : Le Master B conserve le droit d'accorder des autorisations d'accès.

Marche à suivre

AVIS

Perte de données

Si le Master B est inséré pendant **15 s**, la réinitialisation INI commence.
La réinitialisation INI efface tous les réglages et données stockés dans le composant.

Master B  	Insérer le Master B dans le cylindre pendant environ **10 s**. -> 1 signal long et 2 signaux courts retentissent (à partir de la version 42 du micrologiciel). -> (Avant la version du micrologiciel 42 : 2 signaux courts retentissent.) -> Tous les droits d'accès attribués par le Master B ont été annulés.	À partir de la version du micrologiciel 42 : 1x long 1x court
		Avant la version du micrologiciel 42 : 2x court

7.4.3 Réinitialisation INI avec des médias master

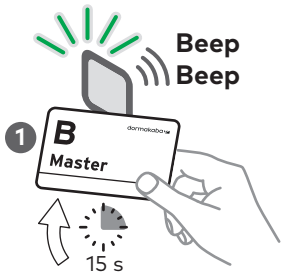
Effets de la réinitialisation INI

- Les paramétrages et données sont supprimés et réinitialisés sur les valeurs de départ (paramètres d'usine).
- Le point d'accès est bloqué durant la réinitialisation INI.
- Toutes les autorisations d'accès, les médias master et le Traceback sont effacés.
- Le point d'accès est bloqué après la réinitialisation INI.

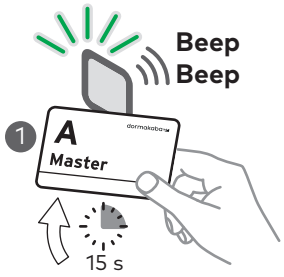
7.4.3.1 Cartes

7.4.3.1.1 Whitelist

Dans une structure master B

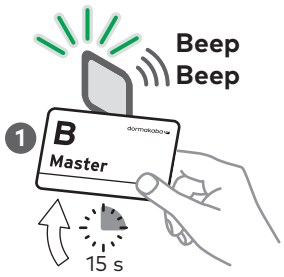
Réinitialisation INI avec Master B		
	Maintenir le Master B env. **15 s**devant l'unité de saisie. -> Le voyant vert s'allume. -> Les signaux ci-contre retentissent. -> Après 15 s, la réinitialisation INI est exécutée. -> Le vert s'éteint.	après 10 s : 1x long, 1x court, après 15 s, 2x court

Dans une structure master A/B

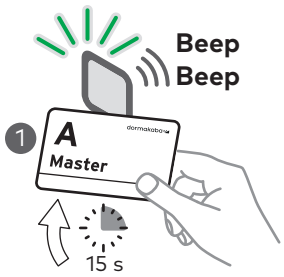
Réinitialisation INI avec Master A		
	Maintenir le Master A env. **15 s** devant l'unité de saisie. -> Le voyant vert s'allume. -> Les signaux ci-contre retentissent. -> Après 15 s, la réinitialisation INI est exécutée. -> Le vert s'éteint.	après 10 s : 1x long, 1x court, après 15 s, 2x court

7.4.3.1.2 CardLink

Avec Master B

Réinitialisation INI avec Master B		
	Maintenir le Master B env. **15 s**devant l'unité de saisie. -> Le voyant vert s'allume. -> Après 15 s, la réinitialisation INI est exécutée. -> 2 signaux courts retentissent. -> Le vert s'éteint.	2x court

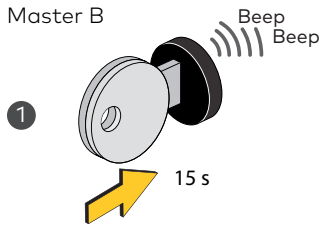
Avec Master A

Réinitialisation INI avec Master A		
	Maintenir le Master A env. **15 s** devant l'unité de saisie. -> Le voyant vert s'allume. -> Après 15 s, la réinitialisation INI est exécutée. -> 2 signaux courts retentissent. -> Le vert s'éteint.	2x court

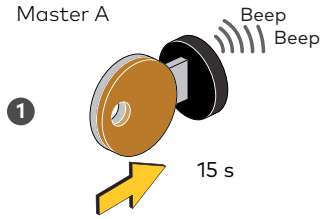
7.4.3.2 Clé

7.4.3.2.1 Whitelist

Dans une structure master B

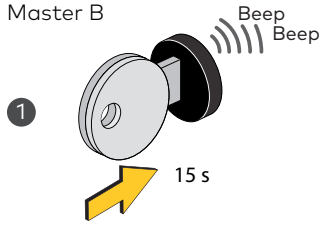
Réinitialisation INI avec Master B		
	Insérer le Master B dans le cylindre pendant env. **15 s**. -> Les signaux ci-contre retentissent. -> Après 15 s, la réinitialisation INI est exécutée.	après 10 s : 1x long, 1x court, après 15 s, 2x court

Dans une structure master A/B

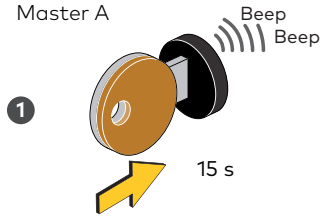
Réinitialisation INI avec Master A		
	Insérer le Master A dans le cylindre pendant env. **15 s**. -> Les signaux ci-contre retentissent. -> Après 15 s, la réinitialisation INI est exécutée.	après 10 s : 1x long, 1x court, après 15 s, 2x court

7.4.3.2.2 CardLink

Avec Master B

Réinitialisation INI avec Master B		
	Insérer le Master B dans le cylindre pendant env. **15 s**. -> Après 15 s, la réinitialisation INI est exécutée. -> 2 signaux courts retentissent.	2x court

Avec Master A

Réinitialisation INI avec Master A		
	Insérer le Master A dans le cylindre pendant env. **15 s**. -> Après 15 s, la réinitialisation INI est exécutée. -> 2 signaux courts retentissent.	2x court

7.5 Programmation avec logiciel système

Avec ce mode de programmation, les données configurées dans le logiciel système sont transférées aux composants à l'aide du Programmer ou via wireless. Les médias master de l'installation de fermeture sont absolument nécessaires pour ce mode de programmation. En

mode wireless, les médias master sont nécessaires pour la mise en service des composants. La programmation de fonctions temps et la lecture du Traceback (mémoire d'événements) sont possibles avec ce mode de programmation.

Les composants et les médias sont gérés et les autorisations sont attribuées avec le logiciel système. Dans ce cadre de nombreuses conditions organisationnelles, structurelles et personnelles peuvent être représentées et tous les mouvements peuvent être retracés.

7.5.1 Logiciel système pour les composants evolo

Selon le domaine d'utilisation et la taille de l'installation, différents logiciels système sont utilisés.

7.5.2 Programmation avec logiciel système et programmeur

Marche à suivre

- Configurer l'appareil dans le logiciel système.
- Transmettre la configuration sur le programmeur.
- Tenir le média master environ 1 s devant l'unité de saisie.
- Connecter le programmeur à l'appareil.
- Transmettre la configuration du programmeur à l'appareil.

Voir aussi :

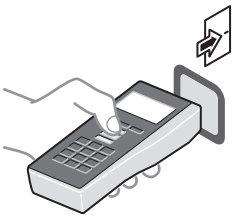
- Description du système
- Documentation du logiciel système utilisé
- Manuel d'utilisation Programmer 1460
- Directive de planification Wireless

7.5.3 Exportation vers des composants

Lors de l'exportation, les données de configuration sont transférées du Programmer vers les composants.

Pour l'exportation, les données de configuration des plans de fermeture doivent d'abord être transférées du logiciel système au Programmer.

7.5.3.1 Exportation des composants dans evolo



Sélectionner les données de configuration dans la liste du programmer et les transférer vers les composants.

✓ Média master valide disponible

1. Appuyer sur la touche menu Exportation.
   ⇨ Le menu Exportation s'ouvre.
2. Enregistrer le Master au composant.

Activer l'électronique de la serrure d'armoire 21 10 en appuyant brièvement sur la porte.

3. Sélectionner le plan de fermeture.
4. Appuyer sur la touche ENTER.
5. Sélectionner la porte.
6. Appuyer sur la touche ENTER.

7.5.4 Importation à partir des composants

Activer l'électronique de la serrure d'armoire 21 10 en appuyant brièvement sur la porte.

Lors de l'importation, les données de configuration sont transférées dans le Programmer à partir des composants. Le Programmer est ensuite connecté à un PC afin de poursuivre le traitement des données avec un système hôte, par exemple avec une analyse Traceback ou la création d'un paquet de support destiné à faciliter l'analyse des erreurs par le support.

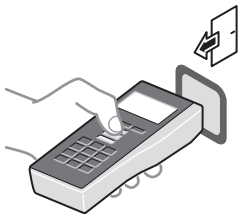
Les données suivantes sont disponibles :

- Information (données d'état)
- Traceback
- Configuration
- Mise à jour CardLink
- Analyse des données

Les données de configuration existantes des composants sont écrasées sur le Programmer après la confirmation.

Le Traceback et la configuration doivent être transférés au logiciel système pour évaluation avec le Programmer.

7.5.4.1 Importation à partir du cylindre digital, de c-lever et du lecteur



✓ Média master valide disponible

1. Appuyer sur la touche menu Importation.
   ⇨ Le menu Importation s'ouvre.
2. Enregistrer le Master au composant.

Activer l'électronique de la serrure d'armoire 21 10 en appuyant brièvement sur la porte.

3. Choisir le menu, par exemple Configuration.
4. Appuyer sur la touche ENTER.

⇨ La configuration du composant est lue et confirmée.

7.6 Mobile Access

7.6.1 Configuration requise du système

Firmware/Logiciel système

Fonction	Micrologiciel	Logiciel système		
		Kaba exos 9300	**MATRIX**	**KEM**
Mobile Access	Voir chapitre Validité > Option Mobile Access	À partir de la version 4.0.73	MATRIX Professional À partir de la version 3.2.x, avec option Mobile Access	À partir de la version 6.0

			MATRIX ONE À partir de la version 3.7	

7.6.2 Initialisation de l'appareil pour Mobile Access

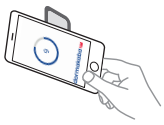
Conditions préalables

Général	• L'installation de contrôle d'accès est établie par dormakaba auprès de Legic Connect
Logiciel système	• La version installée du logiciel système prend en charge Mobile Access. • Une connexion à Legic Connect est établie. • L'appareil est configuré pour Mobile Access dans le logiciel système. • La configuration est transmise sur le programmeur.
Périphérique	• L'appareil est installé et prêt à fonctionner. • La technologie de média est définie, voir chapitre Définir la technologie de média • La configuration est transmise du programmeur à l'appareil.
Smartphone	• VCP Installer est installé et enregistré auprès de Legic Connect avec le numéro de téléphone. Le code d'enregistrement obtenu par SMS a été saisi. • L'accès à Internet est possible (WiFi ou données mobiles). • Le mot de passe pour le fichier VCP est connu.

Marche à suivre

Clé Bluetooth/NFC transmise à l'appareil

- Tenir le média master environ 1 s devant l'unité de saisie.
- Démarrer l'installateur VCP sur le smartphone.
- Sélectionner le fichier VCP.
  - Si le fichier VCP souhaité n'est pas présent, sélectionner 'Actualiser'. Le smartphone télécharge ensuite le fichier VCP .
- Appuyer sur « Envoyer ».
- Saisir le mot de passe pour le fichier VCP.



- Tenir le smartphone devant l'appareil de lecture.

Signalisation / Affichage		
	Périphérique / Unité de saisie	**Smartphone**
Pendant la transmission de données :	• Le voyant vert s'allume.	
Après une initialisation réussie :	• 3 signaux sonores retentissent.	• Vert • Numéro de série de l'appareil
L'appareil est initialisé.		
Après une initialisation non réussie :	• 1 signal court retentit.	• Rouge

Signalisation / Affichage		
	Périphérique / Unité de saisie	**Smartphone**
	• Le voyant s'allume brièvement en rouge. • 1 signal long retentit. • Le voyant s'allume brièvement en rouge. • 1 signal court retentit.	

7.6.3 Initialisation de l'appareil pour evolo smart

L'app evolo smart guide l'utilisateur à travers le processus d'initialisation des composants.

7.6.4 Régler la puissance du signal Bluetooth

Ne modifier les valeurs par défaut que si cela est indispensable.

- Appareils sans connexion sans fil :
  Régler la puissance du signal Bluetooth dans le système de niveau supérieur et l'appliquer à l'appareil à l'aide du programmeur.
- Appareils avec connexion Wireless :
  Régler la puissance du signal Bluetooth dans le système parent et l'appliquer au périphérique à l'aide du hub de communication.

Voir aussi directive de planification Mobile Access.

7.7 Initialisation des composants wireless

Une mise en service wireless doit être effectuée pour que les composants puissent fonctionner en mode wireless.

Pour plus d'informations sur wireless, voir la directive de planification wireless et le manuel technique du hub de communication 90 40-K7.

Conditions préalables

- La passerelle réseau en question est créée et configurée dans le logiciel système.
- Le composant est créé dans le logiciel système.
- Le composant est configuré pour un fonctionnement Wireless.

En cas d'utilisation de plusieurs hubs de communication, toujours lancer la mise en service wireless sur un seul hub de communication.
Les composants pourraient sinon se connecter à un hub de communication indésirable.

Lancer la mise en service wireless sur le hub de communication :
Via l'interface web

1. Sélectionner le hub de communication pour la mise en service dans le gestionnaire de fichiers.
2. Démarrer l'interface web du hub de communication.
3. Appeler la fonction « Mise en service wireless ».
4. Régler la période de mise en service.
   ⇨ Pendant cette période, les composants peuvent être connectés au hub de communication.
5. Démarrer la mise en service wireless.

Via le logiciel système

✓ Le hub de communication pour la mise en service est créé et configuré dans le logiciel système.

1. Dans le logiciel système, sélectionner le hub de communication pour la mise en service.
2. Appeler la fonction « Mise en service wireless ».
3. Régler la période de mise en service.

⇨ Pendant cette période, les composants peuvent être connectés au hub de communication.

4. Démarrer la mise en service wireless.

Si tous les composants nécessaires n'ont pas pu être mis en service pendant la période définie, le processus peut être répété. Les composants déjà connectés au hub de communication restent connectés.

Connecter des composants

✓ La passerelle réseau a été créée.

✓ La configuration wireless du composant a été transférée au Programmer ou le composant est déjà configuré pour le mode wireless.

✓ La mise en service Wireless sur la passerelle réseau a commencée.

1. S'enregistrer au composant avec le média master.
2. Dans le Programmer, ouvrir le menu "Paramètres de l'actuateur".
3. Sélectionner le sous-menu Wireless.
4. Sélectionner **Connecter**.
5. Confirmer avec ENTER.
   ⇨ Connexion à GW ... (Recherche de réseau.)
   ⇨ Passerelle réseau (GW) trouvée.
   ⇨ Connecter au GW est effectuée.
   ⇨ Mise en service ...
   ⇨ Connecté à GW.

⇨ La mise en service wireless du périphérique est terminée.

7.8 Réglage des propriétés et des fonctions d'un composant

Avec le programmer, les propriétés suivantes d'un composant peuvent être modifiées :

- La date et l'heure de l'horloge.
- L'affichage visuel et la signalisation acoustique.
- La durée d'ouverture (valeur par défaut 6 s).
- La version du micrologiciel.
- La réinitialisation INI.
- Connecter un composant wireless à une Wireless Gateway.

Fonctions principales
Les deux fonctions principales qui peuvent être exécutées sur les composants avec le programmer sont **Exporter** et **Importer** des données. Ces deux fonctions sont exécutées avec le programmer via l'interface radio (NFC) ou avec le câble de programmation.

7.9 Réinitialisation (INI-Reset)

Une réinitialisation INI permet de remettre les composants dans leur état initial.

AVIS

Perte de données

Lors d'une réinitialisation INI, tous les réglages et données enregistrés jusque là sur le module électronique sont supprimés.

La connexion à la passerelle réseau est interrompue pour les composants wireless.

Pour cela, les possibilités suivantes sont à disposition :

Réinitialisation avec médias master
Une réinitialisation INI est effectuée lorsque le média master correspondant est présenté aux composants devant l'unité de saisie.

Réinitialisation avec le Programmer 1460
Une réinitialisation INI peut également être effectuée avec le Programmer. Pour cette variante, le média master correspondant est également nécessaire.

Réinitialisation avec pincette et médias master valides
Certains composants disposent de contacts de réinitialisation INI sur le module électronique. Court-circuiter ces contacts avec une pincette conductrice et une réinitialisation INI sera effectuée.

Réinitialisation avec commutateur DIP
Certains composants disposent d'un commutateur DIP. Activer le commutateur DIP spécifique et une réinitialisation INI sera effectuée.

Des informations complémentaires sur la réinitialisation INI figurent dans la documentation du composant.

7.9.1 Vue d'ensemble des variantes INI-Reset des composants

Le tableau suivant présente les variantes INI-Reset et les différences pour E300 (V4) et V3.

Certains composants disposent de contacts INI-Reset. Court-circuiter ces contacts avec une pincette conductrice pendant env. 3 secondes pour effectuer un INI-Reset.

Composant	Master admin.	Programmer 1460[1]	Pincette	Commutateur DIP
c-lever	✓	✓	✓	—
c-lever pro	✓	✓	✓	—
c-lever pro TouchGo	✓	—	✓	—
c-lever compact	✓	✓	—	—
Cylindre digital	✓	✓	✓[2]	—
Cylindre mécatronique Têtière	✓	✓	—[4]	—
Cylindre mécatronique En applique/ Compact	✓	✓	✓[2]	—
Lecteur distant	✓	✓	—	✓[3]
Lecteur compact	✓	✓	—	✓[3]
Serrure d'armoire 21 10	✓	✓[2]	✓	—

Légende :

1 Présenter le média master.
2 Présenter le média master ou un média utilisateur autorisé.
3 Placer le commutateur DIP 6 sur ON.
4 Points de réinitialisation dans le module de têtière

Les informations relatives à la réinitialisation d'autres composants sont décrites dans les manuels des composants.

Toujours effectuer un INI-Reset conformément au manuel de l'appareil.

7.10 Économiser de l'énergie

Composants autonomes
La quantité d'énergie dans la pile et la consommation d'énergie déterminent combien de temps les composants autonomes peuvent fonctionner avant que l'alimentation en énergie ne soit épuisée. Divers réglages permettent d'économiser de l'énergie.

7.10.1 Désactiver les fonctions

Désactiver les fonctions inutiles pour économiser de l'énergie.

En fonction du type de périphérique et de l'utilisation, il est possible de désactiver une ou plusieurs fonctions si elles ne sont pas requises pour l'utilisation prévue. Ceci contribue à économiser de l'énergie et à prolonger l'intervalle entre 2 changements de pile.

Exemples de fonctions pouvant être désactivées :

- Signalisation acoustique (buzzer)
- Signalisation optique (signal lumineux)
- Traceback des médias
- Technologies non requises
- Fonction wireless (si elle n'est pas utilisée)
- Réduire la puissance d'émission wireless, si possible.
- Mobile Access (s'il n'est pas utilisé)

7.10.2 Fonction Object in Field

Le composant vérifie à intervalles réguliers si un média se trouve dans le champ de l'unité de saisie. Pour économiser de l'énergie, l'intervalle entre deux vérifications est prolongé. Avec "Object in Field" dynamique, cette période est étendue pas à pas jusqu'à la valeur maximale. Lors de la présentation d'un média, le processus recommence. Lors de la présentation d'un média, un temps de réaction plus long est possible.

La fonction "Object in Field" (OIF) est paramétrée dans le logiciel système.

Tableau : Économies d'énergie grâce à une OIF dynamique. Les valeurs sont approximatives. Les économies d'énergie effectives dépendent toujours d'autres facteurs et paramètres.

Application concrète	**Paramètres**		**Économie**	**Effets**
Exemples	**OiF Intervalle**	**Dyn. OiF**	**maximum**	
Réglage par défaut du composant. **Accès très fréquentés**	300 ms	DÉSACTIVÉ	0 %	Normal
Accès peu fréquentés	300 ms	ACTIVÉ 30 min	15 %	Temps de réaction prolongé pour le premier média présenté après une pause plus longue. Normal pour les autres médias au sein du temps configuré.
• Respectivement 20 processus matin et soir dans les limites du temps configuré. Le reste du temps, pendant 10 heures, 1 opération par heure.	300 ms	ACTIVÉ 30 min	19 %	
• Pendant 10 heures 1 processus par heure	300 ms	ACTIVÉ 30 min	22 %	
Accès rarement utilisés • 2 processus le matin et 2 le soir pendant le temps configuré. Entre-temps, pas de processus.	300 ms	ACTIVÉ 30 min	30 %	Temps de réaction prolongé lors de la première utilisation après une pause plus longue. • La lecture d'un média présenté peut prendre jusqu'à 1 s.
• Longues périodes de repos entre les opérations • un ou plusieurs jours aucune action	1 000 ms	DÉSACTIVÉ	34 %	

8 Signaux

Ce chapitre décrit les deux types de signaux, leur signification et les messages correspondants.

Des signaux acoustiques et des affichages visuels sont émis lorsque des médias sont détectés par l'unité de saisie du composant.
Les signaux et affichages pour l'autorisation d'accès peuvent être activés ou désactivés individuellement avec la chaîne d'outils.

Symboles

Symboles		Description
		Signal acoustique
		Signal optique

8.1 Durée du signal

Lors de la présentation de médias utilisateurs avec une autorisation d'accès, les signaux acoustiques (bip) et les affichages visuels (LED) suivants sont émis.

Signaux / affichages	Durée	Durée
Bip / LED allumée	très court	40 ms
Bip / LED allumée	court	120 ms
Bip / LED allumée	long	600 ms
Bip / LED allumée	très long	3000 ms

8.2 Autorisations d'accès

Les composants et les médias sont initialisés et programmés.

Messages de service :

Signification			Médias
Autorisé (Ouvrir)	1x court	1x court vert	Médias utilisateurs
Non autorisé (Ne pas ouvrir)	4x court	4x court rouge	Médias utilisateurs
Autorisé (Fermer) [3]	1x court	1x court vert 1x long rouge	Médias utilisateurs
Autorisé (Fermer) [2, 3]	1x court 1x long	—	Médias utilisateurs

Légende :

[1] Les signaux et les affichages peuvent être activés ou désactivés avec la chaîne d'outils (avec le logiciel système (p. ex. KEM) et le programmer).

[2] Composants sans affichage visuel.

[3] Fermer avec des médias autorisés ou actionner la touche (c-lever), par ex. pour le mode Office, Escape Return et le mode Pass.

8.3 Autorisations Pass-Lock (c-lever)

Signification			Médias
Activer	1x long	—	Médias utilisateurs

Signification			Médias
Désactiver (Fermer)	1x court	—	Médias utilisateurs
État (Ouvert)	—	orange très court toutes les 3 s	Médias utilisateurs

8.4 Autorisations Escape Return et Mode Pass (c-lever)

Signification			Activité
Activer	1x long	1x orange très long (3 s)	Appuyer sur la touche pendant 2 s
Désactiver (Fermer)	1x long	5x orange très court	Appuyer sur la touche pendant 2 s
Autorisé (Fermer)	1x court	1x court vert 1x long rouge	Médias utilisateurs
État (Ouvert)	—	1x orange très long (3 s)	Appuyer brièvement sur la touche
État (Non ouvert)	—	5x orange très court	Appuyer brièvement sur la touche

8.5 Messages lors de l'utilisation de la carte de sécurité C2

Lors de l'utilisation de la carte de sécurité C2, les signaux acoustiques et les affichages visuels suivants sont générés.

Indication : L'autorisation d'écriture est supprimée avec la réinitialisation INI.

Utilisation de la carte de sécurité C2 :

Séquence			Médias
Démarrage : Initier les composants	1x court	vert, tant que le média master se trouve dans le champ de l'unité de saisie	Master A ou Master B
Programmer l'autorisation d'écriture.	—	vert, tant que le processus n'est pas terminé	Maintenir la carte de sécurité C2 dans le champ de l'unité de saisie pendant 15 s
Fin : La programmation de l'autorisation d'écriture est terminée	3x bref	—	—
Effacement de l'autorisation d'écriture de la carte de sécurité C2	3x bref	—	—

8.6 Messages de programmation

Messages lors de la programmation :

Séquence			Médias
Démarrage : Médias à programmer	1x court	La LED s'allume lorsque des médias se trouvent à dans le champ de l'unité de saisie. Elle ne s'allume pas lorsqu'un signal acoustique est émis.	Master A et Master B
Confirmation des médias programmés[2]	1x court		Master A et Master B
Média effacé[2]	après 3 s 2x court		Médias utilisateurs
Tous les médias effacés[2]	après 10 s[3] 2x court		Master B (dans structure A/B)
	après 10 s[4] 1x long 1x court		
Fin : Médias à programmer	1x long		Master A et Master B
Erreur lors de la programmation	1x long	1x bref rouge	
Erreur lors de la programmation[1]	2x long	—	

Légende:

[1] Composants sans affichage visuel

[2] Uniquement pour mode Whitelist sans système hôte

[3] Avant la version du micrologiciel 42

[4] À partir de la version du micrologiciel 42

8.7 Composants

Signification			Outil
Identifier les composants[6]	1x court	1x long vert 1x court vert	

Légende:

[6] Le signal est répété toutes les 3 s jusqu'à ce que le processus prenne fin.

8.8 Messages de réinitialisation

Indication : L'autorisation d'écriture est supprimée avec la réinitialisation INI.

Signification			**Outil**
Confirme la réinitialisation	après 3 s 2x court	—	Pincette Court-circuiter les contacts de réinitialisation INI
Confirme la réinitialisation (Whitelist)	après 10 s 1x long 1x court après 15 s 2x court		Médias master
Confirme la réinitialisation (CardLink)	après 15 s 2x court		Médias master
Confirme la réinitialisation	2x court		Programmer 1460

8.9 Messages d'erreur et de dysfonctionnement

Signification			Médias
Pile « faible » FW 42.XX	1x très court	9x rouge très court[3]	Médias utilisateurs Master A et Master B
Pile « faible » FW 42.XX[1]	9x très court[3]	—	Médias utilisateurs Master A et Master B
Pile « vide »	1x très long[3]	—	Médias utilisateurs Master A et Master B
L'autotest n'a pas pu être mené à terme[5]	8x court	8x court rouge	Médias utilisateurs
Médias non autorisés[4]	4x court	4x court rouge	Médias utilisateurs
Panne de l'horloge propre dans le composant[2]	1x long 1x court 1x long	1x court vert	Médias utilisateurs Master A et Master B
Toutes les sitekeys n'ont pas pu être créées	1x court 1x long 1x court	2x court rouge	Master A et Master B (MIFARE)
Toutes les clés de l'installation n'ont pas pu être créées			Médias de service

Légende :

1 Composants sans affichage visuel.

2 Condition, l'horloge a été réglée correctement auparavant.

3 Puis 1x court vert et le composant s'ouvre.

4 Pile « faible » n'est pas signalée.

5 Fonction uniquement pour c-lever, les cylindres mécatroniques et digitaux.
Remarque : Il est recommandé d'effectuer un contrôle d'état sur les composants respectifs.

9 Maintenance du système

9.1 Plan de maintenance



AVIS

Danger pour les composants électroniques dû à une décharge électrostatique.

Une manipulation incorrecte des cartes de circuits imprimés ou des composants électroniques peut entraîner des dommages pouvant conduire à une panne totale ou à des erreurs sporadiques.

- Lors de l'installation et de la réparation du produit, les mesures générales de protection ESD doivent être respectées.

Effectuer les tâches suivantes pour pouvoir utiliser les installations de fermeture et les composants sans problème pendant longtemps.

Les informations détaillées relatives aux opérations de maintenance figurent dans les manuels d'utilisation des composants correspondants.



Les informations sur les périodes de maintenance et l'espérance de vie des pièces ou des composants peuvent varier en fonction des contraintes et des conditions ambiantes.
Les valeurs indiquées se rapportent à une sollicitation moyenne.

Vérification

- Effectuer un contrôle fonctionnel du composant tous les 12 mois, conformément au manuel.
- Vérification et réglage de l'heure avec le Programmer 1460 tous les 12 mois.
  En fonctionnement wireless, la synchronisation de l'horloge s'effectue via le hub de communication.

Mise à jour

Effectuer une mise à jour du micrologiciel pour adapter les fonctionnalités chaque année ou selon les besoins. Éviter que différentes versions du micrologiciel soient installées sur les composants d'une installation.

Remplacer les piles

Les tableaux suivants présentent les intervalles moyens auxquels les piles des composants doivent être remplacées. La durée de vie moyenne dépend du type de pile et des conditions ambiantes. Elle dépend également de la configuration utilisée (Whitelist/CardLink), de l'équipement (autonome/wireless) et des options paramétrées (par ex. signalisation acoustique).

Contrôler l'état de la pile tous les 12 mois. Le cas échéant, remplacer les piles.

- Conditions ambiantes : Voir les spécifications du fabricant des piles.
- Type de pile : lithium. Utiliser uniquement les types de piles recommandés.

9.2 Durée de vie des piles

La durée de vie d'une pile en tant que source d'énergie pour des composants autonomes dépend de nombreux facteurs.

- Variations de qualité du fabricant de piles.
- Type de fonctions utilisées d'un composant.
- Nombre de fonctions utilisées et/ou combinées d'un composant.
- Nombre d'opérations dans une période donnée, par ex. par jour/semaine/mois/année.
- Conditions ambiantes telles que température, humidité de l'air, etc.

Le composant signale un faible niveau de charge de la pile.

Exemples de durée de vie des piles des différents composants :

Hypothèses pour le tableau :

- Température moyenne 20 °C
- Fonctionnement autonome
- Type d'accès Whitelist
- Sans signalisation acoustique

Composant	Actionnements par jour ouvré	Intervalle
c-lever pro	env. 250	24 mois
c-lever		
c-lever compact	env. 100	24 mois
Cylindre digital	env. 100	12 mois
	max. 50	24 mois
Cylindre mécatronique, variante à têtière	env. 400	12 mois
	env. 100	24 mois
Cylindre mécatronique, variantes - Compact - En applique	env. 50	24 mois
Serrure d'armoire 21 10	env. 100	24 mois

Piles dans les médias TouchGo :

Composants	Type de pile	Tension	Type	Plage de température	Durée de vie
Porte-clés	CR2450	3 V	Lithium	-20 à 65 °C	env. 1 an
Bracelet	CR2450	3 V	Lithium	-20 à 65 °C	env. 1 an
Porte-carte	CR2430	3 V	Lithium	-20 à 65 °C	env. 1 an

9.3 Période tampon pour le remplacement des piles

Lors du remplacement des piles, il convient de noter que vous ne disposez que de peu de temps avant que les réglages de l'horloge des composants ne soient perdus (voir le tableau suivant).

Remarque : Vérifier les réglages de l'horloge des composants après le remplacement des piles.

Temps tampons :

Composants	Temps tampon
c-lever	< 60 s
c-lever pro	< 45 s
c-lever compact	< 45 s
Cylindre digital	< 45 s
Cylindre mécatronique • Têtière • Compact • En applique	< 45 s
Serrure d'armoire 21 10	< 120 s

9.4 Ouverture en cas de piles déchargées

Si tous les messages d'alarme ont été ignorés jusqu'au déchargement complet des piles, les composants ne peuvent plus être ouverts qu'avec la fonction d'alimentation d'urgence du Programmer 1460.

Une description de l'alimentation d'urgence (ouverture d'urgence) figure dans le manuel d'utilisation du Programmer 1460.

Pour le cylindre digital et la c-lever compact, la ou les piles se trouvent à l'extérieur. Après le remplacement, vérifier l'horloge du composant avec le Programmer 1460 ou via wireless et la régler si nécessaire.

La serrure d'armoire 21 10 ne comporte pas de fonction d'ouverture d'urgence lorsque la pile est vide. Si la pile est vide, la serrure doit être forcée.

- Remplacer la pile lorsque l'écran affiche « Batterie vide ».

9.4.1 Média d'ouverture d'urgence temporaire

Un média d'ouverture d'urgence est possible à partir de la version du micrologiciel 42.36.

En cas de pile vide et de perte de la configuration, il est encore possible de programmer manuellement un média d'ouverture d'urgence temporaire. Ce média permet d'ouvrir la porte une fois pour changer la pile. L'utilisation du média d'ouverture d'urgence est possible avec

- c-lever
- c-lever pro
- Cylindre MC

Le média d'ouverture d'urgence est programmé à l'aide du média master dans la mémoire RAM du composant et n'est valide que pendant 1 minute ou jusqu'au prochain redémarrage.

Pour la signalisation, voir le chapitre Messages de programmation [▶ 8.6].

Conditions préalables

- Pile faible ou pile vide avec alimentation d'urgence
- Le média master est disponible.
- Le média d'ouverture d'urgence est un média utilisateur spécifique à une installation.
- Mode de fonctionnement : Whitelist
- La Whitelist est vide.

Marche à suivre

1. Présenter le média master.
   ⇨ Signalisation en cas de pile faible : pile faible, suivi du début du mode de programmation
   ⇨ Signalisation avec alimentation d'urgence : Début de la programmation
2. Présenter le média utilisateur prévu comme média d'ouverture d'urgence.
   ⇨ 1 seul média d'ouverture d'urgence est possible
   ⇨ L'enregistrement est signalisé.
3. Présenter le média master.

⇨ Après la fin du processus de programmation, la porte peut être ouverte à l'aide du média d'ouverture d'urgence pendant 1 minute. Ensuite, le média est à nouveau effacé de la mémoire.

9.5 Configurations et Traceback

Le réglage correct des valeurs de la date et de l'heure assure une gestion actuelle des temps avec les composants.

Les composants connectés au logiciel système via la fonction wireless sont mis à jour via la passerelle réseau (par exemple heure, configuration). Le Traceback peut être lu avec le logiciel système.

En fonctionnement purement autonome, les configurations sont transférées ou modifiées (par exemple réglage de l'heure) à l'aide du Programmer.
Le Programmer permet de lire le Traceback et de le transférer au logiciel système pour son évaluation.

Les autres étapes sont décrites dans le manuel d'utilisation du Programmer 1460.

9.6 Mise à jour FW des composants

Le micrologiciel des composants peut être actualisé dans le sous-système evolo.

Les nouvelles versions du micrologiciel sont transférées aux composants autonomes avec le Programmer ou via wireless.

Remarque : Les composants Multi RFID (MRD) avec programmation manuelle doivent être vérifiés pour la programmation manuelle avec les médias appropriés après une mise à jour du micrologiciel. Si nécessaire, effectuer une réinitialisation INI.

Pour certains composants (lecteurs en fonctionnement en ligne), des fonctions peuvent être modifiées par une mise à jour du micrologiciel.

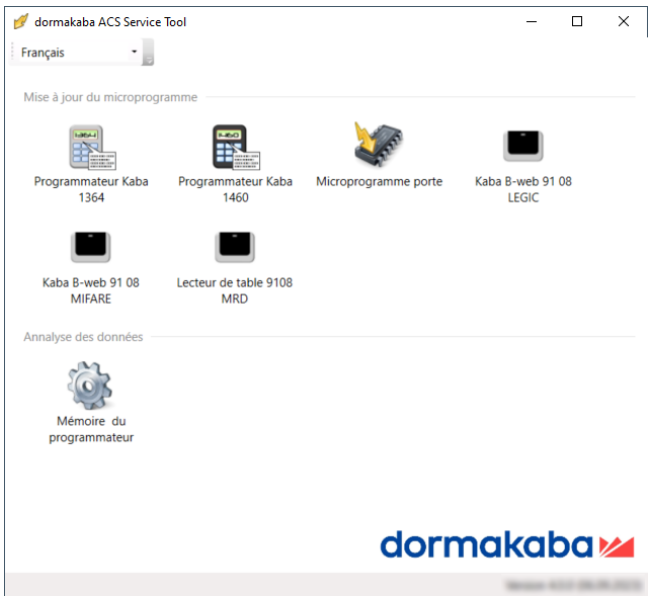
Si le composant comporte des autorisations de lecture/écriture, ce qui suit s'applique à partir du micrologiciel du composant 42.40 et du micrologiciel du programmer 01.36 :
Les autorisations de lecture/écriture (données de lancement) ne sont **pas** effacées par la mise à jour du micrologiciel.
Si les autorisations de lecture/écriture doivent être effacées, il faut effectuer une réinitialisation INI.

Une description détaillée figure dans le manuel d'utilisation du Programmer 1460.

9.7 dormakaba ACS Service Tool

dormakaba ACS Service Tool est un programme auxiliaire permettant de mettre à jour les données du micrologiciel et d'établir des diagnostics.

L'outil peut également être démarré directement, c'est-à-dire sans que le logiciel système soit en cours d'exécution. Pour le lancer, sélectionner *Menu Démarrer -> Programmes -> Kaba -> dormakaba ACS Service Tool*.



Programmer 1364	Assistant de mise à jour du micrologiciel du Programmer.
Programmer 1460	Assistant de mise à jour du micrologiciel du Programmer.
Micrologiciel des actuateurs	Assistant de transfert du micrologiciel des composants sur le Programmer.

Lecteur de table 91 08 LEGIC/MIFARE/MRD	Assistant de mise à jour du micrologiciel du lecteur de table pour la technologie sélectionnée.
Image mémoire Programmer 1460	Assistant de création d'un fichier ZIP avec le contenu de la mémoire du Programmer. Un outil pour résoudre les problèmes en cas de recours au support technique.

Avant la mise à jour, le micrologiciel doit être téléchargé depuis Internet/Extranet sur un disque dur local.

Le Programmer 1364 n'est plus disponible ni pris en charge. Dernier micrologiciel téléchargeable : 1.38

Notes

www.dormakaba.com

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

www.dormakaba.com