

MobileKey

Manuel

09.09.2019

Simons  Voss
technologies

Tables des matières

1	Introduction	4
1.1	Précautions de sécurité	4
1.2	Conditions de système requises.....	5
1.2.1	Administration de l'installation de fermeture	5
1.2.2	Programmation.....	5
2	La matrice.....	7
3	Fonctions de base.....	9
3.1	Créer une serrure	9
3.2	Créer clé.....	10
3.3	Créer un clavier à PinCode.....	10
3.4	Attribuer et sauvegarder une autorisation.....	11
3.5	Attribuer un plan horaire.....	12
3.6	Programmation des composants.....	12
3.6.1	REMARQUE : Programmer via un appareil Windows.....	13
3.6.2	REMARQUE : Programmer via un appareil Android.....	13
3.6.3	REMARQUE : Programmer via un appareil macOS	14
3.7	Réinitialisation de composants.....	15
3.8	Suppression forcée de composants	15
3.9	Lire le compte-rendu des accès.....	15
4	Extension MobileKey ONLINE	17
4.1	SmartBridges	17
4.1.1	Placer les SmartBridges.....	18
4.1.2	Configurer les SmartBridges.....	19
4.1.3	Supprimer SmartBridge	19
4.2	Paramétrer la serrure avec des nœuds de réseau.....	20
4.3	Supprimer la serrure avec des nœuds de réseau.....	21
4.4	Créer un clavier à PinCode en ligne.....	22
4.5	Supprimer un clavier PinCode en ligne.....	23
4.6	Configurer les composants en ligne	24
4.7	Programmation des composants.....	24
4.8	Couper la connexion des composants en ligne	25
4.9	Effectuer une ouverture à distance.....	25
4.10	Key4Friends	26
4.10.1	Partager une clé.....	26
4.10.2	Administrer clé.....	27

4.11	Serrure DoorMonitoring - Affichage des états de la porte	27
5	Gestion des événements	30
5.1	Consulter les messages dans l'application Web	30
5.2	Créer des règles	30
5.2.1	Créer une règle de type « Accès »	30
5.2.2	Créer une règle de type « DoorMonitoring »	31
5.2.3	Créer une règle de type « Alarme »	32
5.3	Remarques importantes	32
6	Aide.....	34
6.1	Aide avec des clés (transpondeurs).....	34
6.2	Aide avec serrures (par ex. cylindre de fermeture)	35
6.3	Réinitialiser ou réutiliser les composants supprimés	36
6.4	Lire les composants.....	37
6.5	Aide concernant SmartBridge	37
6.6	Aide relative au clavier PinCode en ligne.....	38
6.7	Aide concernant les serrures en ligne	38
6.8	Erreur de réseau.....	39
6.9	Réinitialisation manuelle des nœuds de réseau.....	39
7	Maintenance, nettoyage et désinfection.....	40
8	Applications MobileKey	41
9	Déclaration de conformité	42
10	Conseils & Astuces	43
10.1	Raccourci vers l'application Web.....	43
10.2	Utilisation de clés sans clé de programmation USB.....	43
10.3	Paramétrer la langue	44
11	Aide et autres informations	45

1 Introduction

MobileKey est une catégorie de produits indépendante pour les petites installations de fermeture. Jusqu'à 100 clés (*transpondeurs*) et 20 serrures (*cylindres de fermeture et SmartRelais*) sont supportés.



REMARQUE

L'administration du plan de fermeture a exclusivement lieu via l'application Web MobileKey. Cette dernière peut être obtenue sous www.my-mobile-key.com. En cliquant sur « Login app web » vous accédez directement à l'application. Créez un compte utilisateur gratuit afin de pouvoir travailler avec MobileKey.

1.1 Précautions de sécurité



ATTENTION

Un composant de fermeture SimonsVoss mal installé ou mal programmé peut bloquer un accès au niveau d'une porte. SimonsVoss Technologies GmbH décline toute responsabilité pour les conséquences d'installations impropres, comme l'accès impossible à des personnes blessées, les dommages matériels ou d'autres dommages.



REMARQUE

SimonsVoss Technologies GmbH décline toute responsabilité pour les dommages causés aux portes ou aux composants en raison d'une installation impropre.



REMARQUE

Les composants SimonsVoss ne doivent être utilisés qu'aux fins prévues, à savoir l'ouverture et la fermeture de portes. Toute autre utilisation est interdite.



REMARQUE

Les modifications et nouveaux développements techniques ne peuvent pas être exclus et peuvent être mis en œuvre sans préavis.



REMARQUE

Toutes les possibilités d'extension en ligne requièrent l'existence d'un réseau radio MobileKey fonctionnant correctement. Toutes les fonctions en ligne ne peuvent être exécutées que si la connexion Internet est stable et si l'alimentation en électricité est garantie.

1.2 Conditions de système requises

1.2.1 Administration de l'installation de fermeture

Le plan de fermeture peut être **affiché et édité** à l'aide de n'importe quel navigateur standard et ce, indépendamment de toute plateforme. En principe, aucun matériel spécial n'est requis, le terminal doit cependant soutenir un des navigateurs Web suivants dans une version actuelle :

- Microsoft Internet Explorer
- Mozilla Firefox
- Google Chrome
- Apple Safari
- Opera

Une connexion Internet permanente doit en outre exister. Pour les travaux rapides, un accès Internet HighSpeed est indispensable.

1.2.2 Programmation

Les composants de fermeture MobileKey peuvent être programmés à l'aide du stick de programmation USB via les appareils suivants :

■ Appareils Windows

- Système d'exploitation : Windows 7, 8 ou 10.
- Matériel : interface USB pour connexion de la clé de programmation USB.

Aucune configuration spécifique du matériel n'est requise pour la programmation. Le système d'exploitation doit fonctionner de manière stable et correcte.

- Le .NET Framework (au moins version 3.5) actuel de Microsoft doit être installé sur l'ordinateur.

Suivez les instructions de l'application de programmation afin de pouvoir programmer les composants de fermeture MobileKey.

■ Appareils Android

- L'application de MobileKey de Google Play Store doit être installée pour l'utilisation.

Les modifications du plan de fermeture continuent d'être effectuées dans l'application Web MobileKey, via le navigateur.

- Le stick de programmation USB peut au choix être directement connecté à l'appareil Android ou le cas échéant via un câble OTG à commander séparément.

Dans ce cas, l'appareil Android doit supporter la fonction OTG. Si vous n'êtes pas sûr que votre appareil Android supporte la fonction OTG, vous pouvez alors procéder à une vérification au moyen d'une application dans Google Play. Recherchez par exemple « OTG check ».

Attention : ces applications n'ont rien à voir avec la société SimonsVoss Technologies GmbH. La survenance de problèmes ou de dommages n'entraînera donc aucune responsabilité !

Démarrez l'application MobileKey via l'application Web MobileKey afin de programmer les composants de fermeture MobileKey.

■ Appareil macOS

- Système d'exploitation : OS X à partir de 10.11 « El Capitan »
- Matériel : interface USB pour connexion de la clé de programmation USB.

Aucune configuration spécifique du matériel n'est requise pour la programmation. Le système d'exploitation doit fonctionner de manière stable et correcte.

■ En option : en ligne via SmartBridge

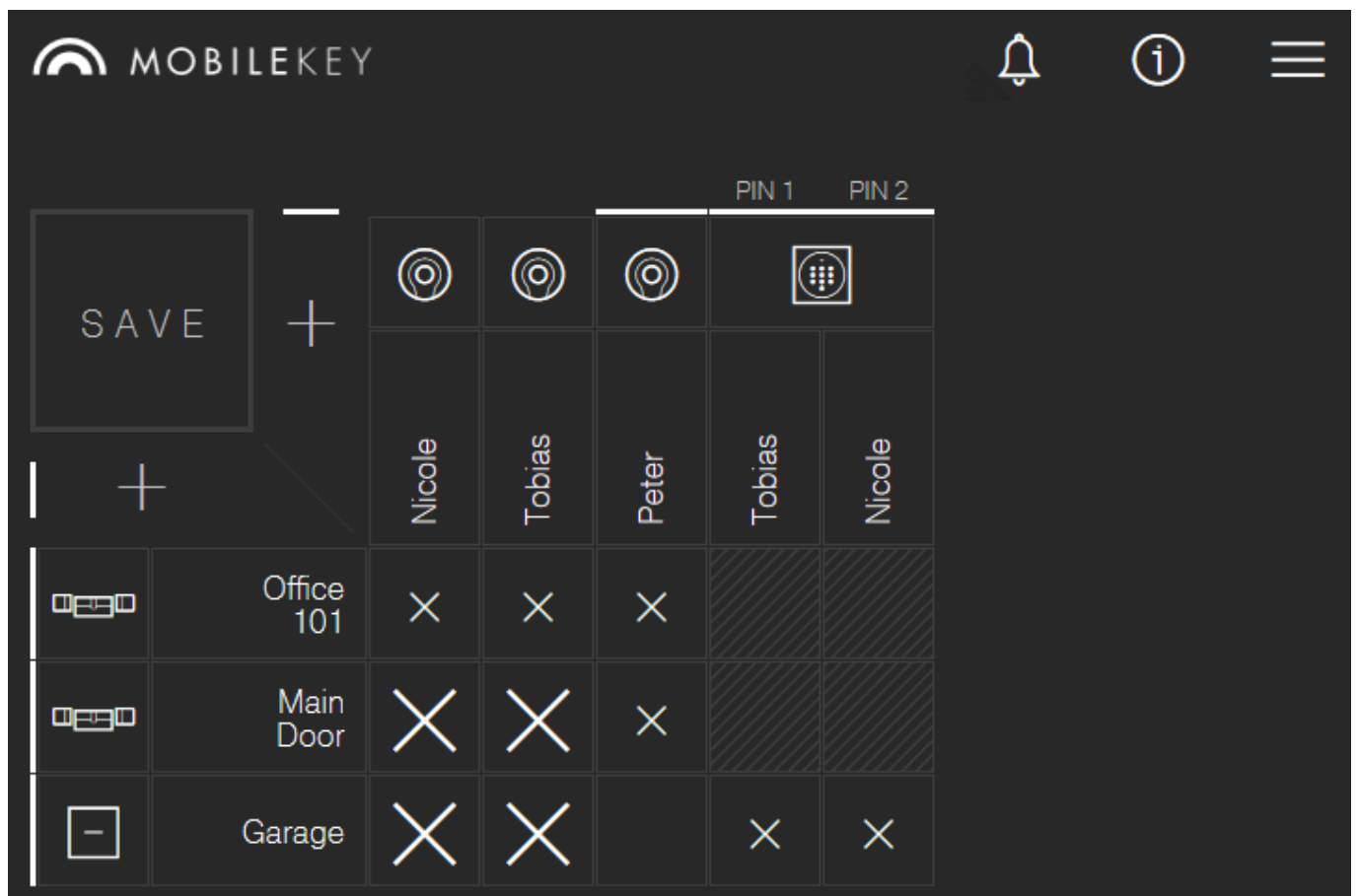
Les serrures peuvent également être programmées en ligne sans clé de programmation USB. Voir *Programmation des composants* [► 24]. Dans ce cas, les transpondeurs doivent être programmés à l'aide de la clé de programmation USB.

Conseil :

*Si aucun appareil Windows ou Android n'est disponible pour la programmation de nouvelles fermetures, il est alors recommandé de programmer d'autres transpondeurs en réserve. Ces derniers pourront être ultérieurement affectés aux serrures en ligne en réseau. Voir *Utilisation de clés sans clé de programmation USB* [► 43].*

2 La matrice

La matrice est l'aperçu général de l'ensemble de l'installation de fermeture. Cet aperçu constitue donc le point central de toutes les autres fonctions. Toutes les clés (par ex. transpondeurs) sont affichées horizontalement et toutes les serrures (par ex. cylindre de fermetures) sont affichées verticalement. Les menus importants sont consultables via les symboles « Centre de messages », « Aide » et « Menu ».



Plusieurs symboles sont utilisés afin de rendre la matrice aussi claire que possible.





Autorisations

SYM-BOLE	DESCRIPTION
×	Croix d'autorisation : Nouveau Autorisation donnée mais non encore programmée.
×	Croix d'autorisation : case cochée L'autorisation a été accordée et est active.
×	Croix d'autorisation : Supprimer L'autorisation a été retirée mais pas encore déprogrammée.

Croix d'autorisation : Aucune autorisation

Si aucune des trois cases précédentes n'est affichée dans ce champ, cela signifie qu'il n'y pas (encore) d'autorisation.

Serrures et clés

SYM- BOLE	DESCRIPTION
	Serrure : Serrure Il s'agit ici d'une serrure ou d'un cylindre de fermeture. <i>Un symbole radio situé dans le coin gauche (en bas) montre si la serrure dispose d'un nœud de réseau pour MobileKey ON-LINE.</i>
	Serrure : SmartRelais Il s'agit ici d'un SmartRelais. <i>Un symbole radio situé dans le coin gauche (en bas) montre si la serrure dispose d'un nœud de réseau pour MobileKey ON-LINE.</i>
	Clé : transpondeur Il s'agit ici d'un transpondeur.
	Clé : Clavier PinCode Il s'agit ici d'un clavier PinCode.

Voir également sur ce point

- ➔ [Aide concernant les serrures en ligne \[▶ 38\]](#)
- ➔ [Aide concernant SmartBridge \[▶ 37\]](#)

3 Fonctions de base

Un assistant apparaît lors de la première connexion au compte MobileKey. Cet assistant vous permet de créer les serrures et clés de manière rapide et confortable.

3.1 Créer une serrure

- ✓ Aperçu de la matrice ouvert
- 1. Cliquez sur le symbole ajouter une serrure (plus en-dessous du bouton SAVE).
- 2. Choisissez le type de serrure par ex. CYLINDRE pour un cylindre de fermeture normal.
- 3. Attribuez un nom par ex. porte d'entrée.
- 4. Cliquez sur le bouton Durée d'ouverture en secondes ou Ouverture permanente.
 - ↳ Si vous avez activé Ouverture permanente, la serrure reste alors couplée jusqu'à ce qu'elle soit de nouveau activée par une serrure ou par ouverture à distance.



ATTENTION

Risque de sécurité en raison d'une ouverture permanente

Une porte ouverte en permanence constitue un risque de sécurité. La société SimonsVoss Technologies GmbH recommande donc de limiter la durée d'ouverture.

- 5. Cliquez sur le bouton ENREGISTRER ou ENREGISTRER + COPIER.
 - ↳ ENREGISTRER enregistre la serrure et revient vers la matrice.
 - ↳ ENREGISTRER + COPIER enregistre la serrure et prépare dans le même temps une autre clé avec les mêmes propriétés.



REMARQUE

Les paramètres réseau étendus seront affichés dès qu'au moins un SmartBridge a été installé et configuré. À l'issue de la première programmation des serrures DM, d'autres options en ligne comme par ex. la valeur « Porte ouverte trop longtemps » seront visibles.



REMARQUE

Avec le **SmartRelais 2**, il est possible d'inverser la **sortie (contact de relais)**. Pour ce faire, un SmartRelais doit être créé et programmé. Ensuite, le paramètre LA CONFIGURATION DE SORTIE avec l'option Inverser sortie sera visible dans les propriétés du SmartRelais. Si vous activez cette option, le SmartRelais 2 devra être reprogrammé.

3.2 Créer clé

- ✓ Aperçu de la matrice ouvert
- 1. Cliquez sur le symbole ajouter une clé (PLUS à côté du bouton SAVE).
- 2. Choisissez le type de clé par ex. TRANSPONDEUR.
- 3. Attribuez un nom par ex. « Hans Müller ».
- 4. Déterminez la validité, le cas échéant.
 - ↳ Valable à partir de : définir la date à partir de laquelle la clé est autorisée dans l'installation de fermeture.
 - ↳ Valable jusqu'à : définir la date jusqu'à laquelle la clé est autorisée dans l'installation de fermeture.
- 5. Cliquez sur le bouton ENREGISTRER ou ENREGISTRER + COPIER.
 - ↳ ENREGISTRER enregistre les clés et navigue avec la matrice.
 - ↳ ENREGISTRER + COPIER enregistre les clés et prépare dans le même temps d'autres clés avec les mêmes propriétés.
- ↳ La nouvelle clé est créée.

3.3 Créer un clavier à PinCode

Ce chapitre décrit l'installation d'un clavier PinCode sans extension en ligne. Si vous avez un clavier PinCode avec extension en ligne, veuillez alors suivre les instructions du chapitre *Créer un clavier à PinCode en ligne* [▶ 22].

- ✓ Le clavier à PinCode déjà configuré, voir Configuration (*Master-Pin et au moins un User-Pin doivent avoir été créés !*)
- ✓ Serrure pour clavier PinCode créée
- ✓ Aperçu de la matrice ouvert
- 1. Cliquez sur le symbole ajouter une clé (PLUS à côté du bouton SAVE).
- 2. Choisir le type « CLAVIER PINCODE ».
- 3. Déterminez la serrure à laquelle le clavier à PinCode devra être utilisé.
- 4. Attribuer un nom au PIN 1 (*correspond au User-Pin 1*) par ex. « Hans Müller ». La case blanche pour PIN 1 est déjà cochée.
- 5. Si souhaité, attribuer nom aux PIN 2 & 3. Activer tout d'abord les cases à cocher blanches afin d'activer les PIN.
- 6. Cliquez sur le bouton « ENREGISTRER » ou « ENREGISTRER + COPIER ».
 - ↳ ENREGISTRER enregistre les clés et navigue avec la matrice.

- ↳ ENREGISTRER + COPIER enregistre les clés et prépare dans le même temps d'autres clés avec les mêmes propriétés.



REMARQUE

Jusqu'à 3 User-Pin peuvent être créés sur le clavier PinCode. Ces User-PINs doivent, lors de l'attribution du clavier PinCode, être activés à une serrure dans l'application Web.



REMARQUE

La modification d'un User-PIN dans un clavier PinCode déjà créé est possible en cliquant sur le clavier respectif (dans la matrice) et en sélectionnant « MODIFIER ».

3.4 Attribuer et sauvegarder une autorisation

Dans la matrice, il est possible d'accorder et de retirer des autorisations.

- Autoriser une clé à une serrure : Cocher le champ vide se trouvant à l'intersection entre la clé et la serrure.

La croix est présentée de façon réduite jusqu'à ce que la nouvelle autorisation ait été programmée. À l'issue de la programmation, la croix remplit entièrement le carré de la matrice.

- Révoquer l'autorisation d'une clé à une serrure : Cliquer sur la croix se trouvant à l'intersection entre la clé et la serrure, afin de retirer cette croix d'autorisation.

La croix est présentée de façon incomplète jusqu'à ce que la nouvelle modification ait été programmée. La croix d'autorisation disparaît entièrement après la programmation réussie.



REMARQUE

Les modifications sont signalées par un contour jaune. Ces dernières doivent obligatoirement être enregistrées (ou acceptées) en cliquant sur le bouton « SAVE » et ce, avant la programmation !



REMARQUE

Toutes les modifications et autorisations doivent être programmées via l'application de programmation avant de pouvoir être actives.

3.5 Attribuer un plan horaire

Cette fonction supplémentaire est optionnelle. Vous ne devez donc pas obligatoirement l'utiliser.

Il existe en principe deux types de plans horaires :

- Hebdomadaire : Des intervalles de temps individuels peuvent être attribués pour chaque jour de la semaine. EXEMPLE : l'intendant n'a accès qu'à certains jours et horaires - par ex. le lundi de 8h00 à 12h00 et le jeudi de 13h00 à 15h30.
- Journalier : Un plan de plages horaires peut être créé pour une semaine entière. EXEMPLE : Le collaborateur John Dorian est autorisé aux serrures du lundi au vendredi de 7h00 à 19h00.

Procédez de la manière suivante afin d'attribuer une clé à un plan horaire :

- ✓ Aperçu de la matrice ouvert
 1. Cliquez sur la clé souhaitée dans l'aperçu de la matrice.
 - ↳ Le menu s'ouvre.
 2. Cliquez sur le bouton PLAN HORAIRE.
 3. Choisissez le type du plan horaire.
 - ↳ Hebdomadaire : Choisir le jour et Créer un intervalle de temps. Il est possible de créer plusieurs intervalles de temps à des jours différents.
 - ↳ Journalier : Cliquer sur Exclusion des week-ends lorsque le plan en doit s'appliquer que du lundi au vendredi. Ensuite un Créer un intervalle de temps. Il est possible de créer plusieurs intervalles de temps.
 4. Cliquez sur le bouton ENREGISTRER.
 - ↳ La clé est sauvegardée.
 - ↳ L'aperçu de la matrice s'affiche.
- ↳ La clé est affectée au plan horaire.



REMARQUE

Lorsqu'un intervalle de temps va au-delà de minuit, il faut alors créer deux intervalles de temps : Un intervalle de temps de « Durée avant minuit jusqu'à minuit » et « De minuit à la durée après minuit ».

3.6 Programmation des composants



REMARQUE

Programmez chaque serrure ou clavier PinCode en ligne avant le montage !

Procéder de la manière suivante afin de démarrer l'application de programmation depuis l'application Web MobileKey et afin de pouvoir effectuer chacune des tâches de programmation :

- ✓ Tâches de programmation existantes (affichées dans la matrice au niveau des composants concernés)
- 1. Cliquez sur le Menu.
 - ↳ Le menu s'ouvre.
- 2. Cliquez sur le bouton PROGRAMMER.
 - ↳ L'application de programmation démarre.
- 3. Vous connectez, le cas échéant.
 - ↳ La liste des tâches affiche les composants avec besoin de programmation.
- 4. Exécutez toutes les tâches.
- 5. Cliquez sur le premier composant afin d'en démarrer la programmation.
- 6. Suivez ensuite les instructions de l'application de programmation.

3.6.1 REMARQUE : Programmer via un appareil Windows

L'application de programmation doit être téléchargée et installée. Le nom d'utilisateur et le mot de passe doivent en outre être saisis. Pour la programmation, le stick de programmation USB doit être connecté à la sortie USB de l'ordinateur.

Il sera fait état de cette installation si vous cliquez sur Menu/Programmer. Le message suivant qui apparaît affiche un lien de téléchargement direct. Installez l'application de programmation. Vous avez besoin de droits d'administrateur pour pouvoir installer l'application de programmation.

Veillez tenir compte des conditions inhérentes au matériel :

Programmation [▶ 5]

Voir également sur ce point

→ *Programmation [▶ 5]*

3.6.2 REMARQUE : Programmer via un appareil Android

Téléchargez l'application gratuite de MobileKey dans Google Play Store et connectez le stick de programmation avec l'appareil Android (le cas échéant via un câble OTG à commander séparément).

Démarrez l'application une fois afin de pouvoir saisir votre nom d'utilisateur et le mot de passe.

Veillez tenir compte des conditions inhérentes au matériel :

Programmation [▶ 5]

Voir également sur ce point

→ *Programmation* [▶ 5]

3.6.3 REMARQUE : Programmer via un appareil macOS

La programmation sous macOS requiert l'installation d'un service. Si ledit service n'est pas installé ou pas encore démarré, vous en serez alors avisé. Dès que le service fonctionne, vous ne devez plus quitter le navigateur. Les appareils avec extension en ligne activée ne doivent pas être programmés. Pour la programmation de clés et de serrures sans extension en ligne, il existe deux possibilités sous macOS.

Veillez tenir compte des conditions inhérentes au matériel :

Programmation [▶ 5]

Programmation dans le menu

La première possibilité est la programmation via le menu. Cette méthode est particulièrement adaptée lorsque peu de clés ou de serrures ont été modifiées.

1. Cliquez sur le composant qui doit être programmé.
 - ↳ Le menu s'ouvre.
2. Cliquez sur le bouton **PROGRAMMER**.
 - ↳ La fenêtre de programmation s'ouvre.
3. Suivez les instructions affichées sur l'écran.
 - ↳ La programmation est terminée.

Programmation avec liste de programmation

La deuxième possibilité est la programmation via la liste de programmation. Cette méthode est particulièrement adaptée lorsque de nombreuses clés ou de serrures ont été modifiées.

- ✓ Aperçu de la matrice ouvert
1. Cliquez sur le Menu.
 - ↳ Le menu s'ouvre.
 2. Cliquez sur le bouton **PROGRAMMER**.
 - ↳ La liste de programmation s'ouvre.
 3. Dans la liste, cliquez sur le composant qui doit être programmé.
 4. Suivez les instructions affichées sur l'écran.
 - ↳ Le composant va être programmé.
 5. Le cas échéant, cliquez sur les composants suivants afin de les programmer.
 - ↳ La programmation est terminée.

3.7 Réinitialisation de composants

Les composants peuvent être facilement réinitialisés. Ensuite, ces derniers se trouvent à l'état par défaut et donc non programmé et peuvent être utilisés dans un autre système de fermeture.

1. Cliquez sur le composant respectif.
 - ↳ Le menu s'ouvre.
2. Cliquez sur le bouton SUPPRIMER.
3. Cliquez sur le bouton PROGRAMMER.
 - ↳ L'application de programmation démarre.
4. Exécutez toutes les tâches.
 - ↳ Le composant est supprimé de la liste lorsque la programmation a été effectuée avec succès.

3.8 Suppression forcée de composants

Lorsqu'un composant défectueux ne peut pas être facilement réinitialisé (voir *Réinitialisation de composants* [▶ 15]), il est quand même possible de le supprimer du plan de fermeture. Une nouvelle suppression du composant entraîne la suppression forcée du composant.

- ✓ Composant déjà supprimé.
 - ✓ Composant préalablement programmé.
1. Cliquez encore une fois sur le composant.
 2. Cliquez sur FORCER LA SUPPRESSION et confirmez la saisie.



REMARQUE

La suppression forcée empêche l'utilisation ultérieure d'un composant (encore) programmé. Cette procédure doit seulement être effectuée sur les composants défectueux !

3.9 Lire le compte-rendu des accès

Chaque accès réalisé avec une clé est consigné dans la serrure. Consigner les fermetures MobileKey jusqu'à 500 accès. Lorsqu'ensuite de nouveaux accès ont lieu, les accès les plus anciens sont écrasés. Pour afficher le protocole d'accès, procédez comme suit :

- ✓ Aperçu de la matrice ouvert
1. Cliquez sur la serrure souhaitée, déjà programmée, dont vous souhaitez lire le protocole.
 - ↳ Le menu s'ouvre.
 2. Cliquez sur le bouton HISTORIQUE DES ACCÈS.
 3. Au besoin, modifiez la période du protocole d'accès.

4. Cliquez sur le bouton **LIRE L'HISTORIQUE**.
 - ↳ La commande Lire le protocole d'accès est envoyée en tant que tâche à l'appli de programmation.
5. Cliquez sur le Menu.
 - ↳ Le menu s'ouvre.
6. Cliquez sur le bouton **PROGRAMMER**.
 - ↳ L'application de programmation démarre.
7. Réalisez la tâche de programmation.
8. Fermez l'appli de programmation.
9. Ouvrez le tableau.
10. Cliquez sur la serrure dont vous souhaitez lire le protocole.
 - ↳ Le menu s'ouvre.
11. Cliquez sur le bouton **HISTORIQUE DES ACCÈS**.
 - ↳ Le protocole d'accès apparaît.

4 Extension MobileKey ONLINE

Un SmartBridge (qui sert d'Access Point) permet de mettre des serrures en réseau afin de communiquer directement avec l'application Web. De nouvelles fonctions peuvent en résulter :

- La programmation des serrures peut être effectuée indépendamment de la plateforme.
- Les états de la porte (ouverte, fermée, verrouillée) peuvent être suivis en temps réel.
- Les listes d'accès des serrures peuvent en principe être lues depuis partout.
- Les clés peuvent ainsi être facilement partagées avec des amis via Key4Friends.
- Des ouvertures à distance peuvent être effectuées via l'application Web.

Des composants spéciaux sont nécessaires pour l'utilisation de ces fonctions :

- SmartBridge : En tant qu'Access Point, il est toujours connecté à Internet.
- Serrure supportant « en ligne » : Toutes les serrures MobileKey peuvent être équipées d'un nœud de réseau spécial (*SmartRelais avec platine correspondante*), afin de pouvoir utiliser la fonctionnalité en ligne. On parle ici de nœuds de réseau. Les serrures avec « configuration DoorMonitoring » disposent en outre de capteur intelligent. Ces serrures peuvent constater les états de la porte (ouverte, fermée, verrouillée) et les transmettre à l'application Web.

4.1 SmartBridges

Au moins un SmartBridge doit faire office d'Access Point. Ce dernier est relié à l'Internet et garantit ainsi la connexion au serveur et à l'application Web.



REMARQUE

Les paramètres étendus du réseau (*par ex. lors de la création d'une serrure*) ne sont affichés que lorsqu'au moins un SmartBridge a été créé.



REMARQUE

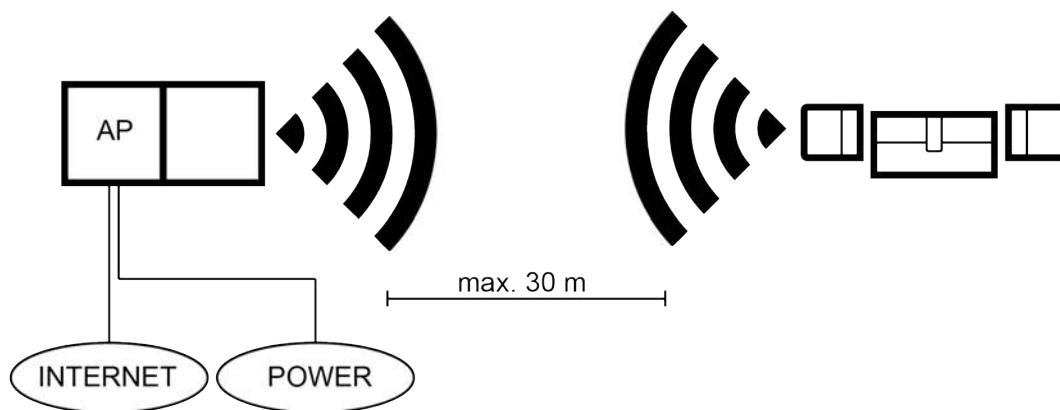
Attention : MobileKey ne permet d'utiliser que 10 SmartBridges au maximum.

4.1.1 Placer les SmartBridges

En fonction de leur utilisation et de leur configuration, les SmartBridges peuvent être utilisés de différentes manières. Les scénarios les plus importants seront présentés ci-après.

4.1.1.1 Un SmartBridge

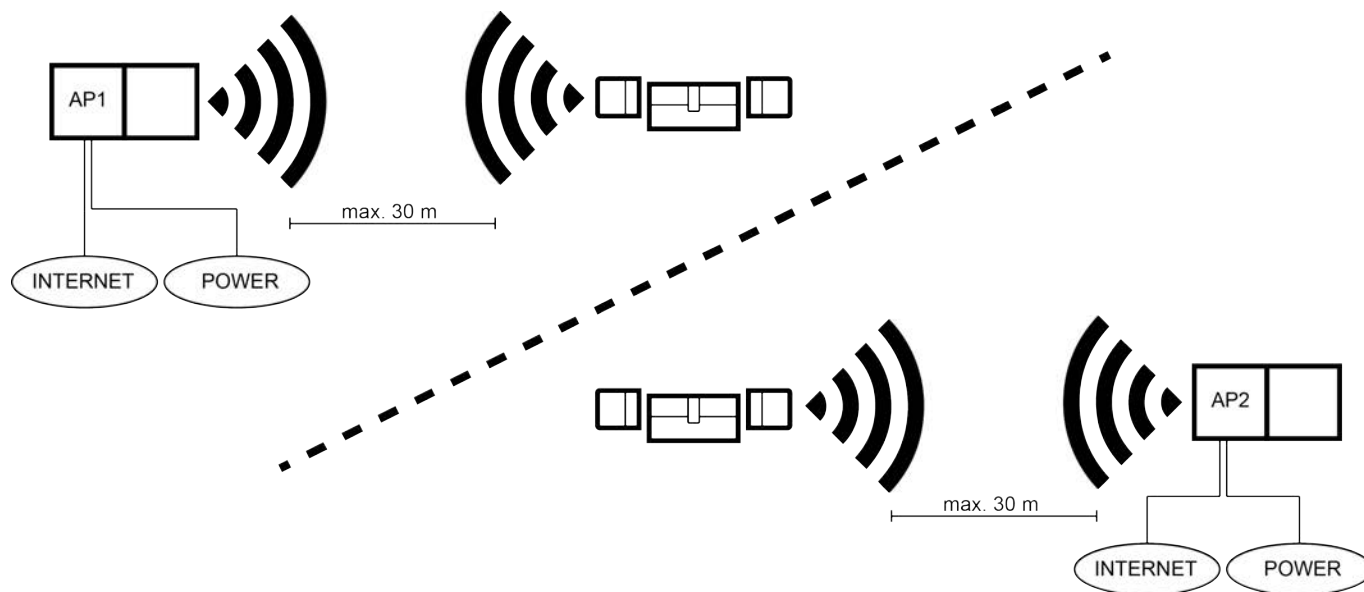
L'utilisation d'un SmartBridge en tant qu'Accesspoint est le mode d'utilisation le plus simple pour MobileKey ONLINE.



4.1.1.2 Deux ou plusieurs SmartBridges

MobileKey ONLINE peut gérer plusieurs Accesspoints. De cette manière, plusieurs sites ou des serrures très éloignées peuvent être couvert(e)s avec le réseau MobileKey ONLINE.

Quelle serrure sera contactée par quel Accesspoint, est décidé automatiquement par MobileKey ONLINE en considération de la puissance du signal. Vous pouvez suivre l'itinéraire de la communication dans le menu RÉSEAU en activant l'option Afficher le SmartBridge attribué.



4.1.2 Configurer les SmartBridges

Voici comment ajouter un nouveau SmartBridge dans l'application Web :

1. Cliquez sur le Menu.
↳ Le menu s'ouvre.
2. Cliquez sur le bouton RÉSEAU.
3. Ajoutez un nouveau SmartBridge en cliquant sur le symbole PLUS des SmartBridges.
↳ Le dialogue concernant l'ajout d'un nouveau SmartBridge démarre
4. Choisissez un type.
↳ Choisissez STANDARD afin de configurer un SmartBridge en tant qu'Accesspoint.
5. Attribuez un nom.
↳ Donnez un nom clair par ex. « SmartBridge Bureau 2 »
6. Saisissez le MobileKey-ID.
↳ Le MobileKey-ID se trouve sur l'emballage ou au dos du SmartBridge.
7. Cliquez sur le bouton ENREGISTRER.
↳ La configuration va être sauvegardée. Vous revenez automatiquement au menu RÉSEAU.

4.1.3 Supprimer SmartBridge



REMARQUE

Les nœuds de réseau des serrures ne peuvent être réinitialisés qu'au moyen du SmartBridge relié. Si la suppression du SmartBridge n'est pas prévue, ce dernier conserve alors sa configuration. Les serrures ne seront toutefois accessibles que via un nouveau SmartBridge ou via l'appareil de programmation.

Voici comment supprimer le SmartBridge dans l'application Web :

- ✓ Les serrures reliées ont le statut « EN LIGNE »
- 1. Cliquez sur le Menu.
 - ↳ Le menu s'ouvre.
- 2. Cliquez sur le bouton RÉSEAU.
- 3. Cliquez sur le SmartBridge à supprimer.
- 4. Cliquez sur le bouton SUPPRIMER.
 - ↳ La suppression du SmartBridge sera alors signalisée.
- 5. Démarrez la configuration du réseau en cliquant sur le bouton « DÉMARRER LA CONFIGURATION ».
- 6. La programmation (dans ce cas la réinitialisation du SmartBridge) est effectuée. Le SmartBridge peut ensuite être à nouveau relié dans chaque installation de fermeture MobileKey.

4.2 Paramétrer la serrure avec des nœuds de réseau



REMARQUE

Les serrures sans fonction en ligne qui sont déjà montées et programmées peuvent être reliées à MobileKey ONLINE ultérieurement. Pour ce faire, le cache de bouton (*cache de bouton intérieur les serrures FD, cache de bouton extérieur pour les serrures CO ou platine supplémentaire pour le SmartRelais*) doit simplement être remplacé par un cache de bouton en ligne avec nœud de réseau. Ensuite le Chip-ID du nouveau nœud de réseau peut être ajouté à la serrure dans l'application Web.

Voici comment ajouter une nouvelle serrure en ligne :

- ✓ SmartBridge créé (*voir Configurer les SmartBridges [► 19]*)
- ✓ Aperçu de la matrice ouvert
- 1. Cliquez sur le symbole ajouter une serrure (plus en-dessous du bouton SAVE).
- 2. Choisissez le type de serrure par ex. CYLINDRE pour un cylindre de fermeture normal.
- 3. Attribuez un nom par ex. porte d'entrée.

**ATTENTION****Risque de sécurité en raison d'une ouverture permanente**

Une porte ouverte en permanence constitue un risque de sécurité. La société SimonsVoss Technologies GmbH recommande donc de limiter la durée d'ouverture.

4. Cliquez sur le bouton Durée d'ouverture en secondes ou Ouverture permanente.
 - ↳ Si vous avez activé Ouverture permanente, la serrure reste alors couplée jusqu'à ce qu'elle soit de nouveau activée par une serrure ou par ouverture à distance.
5. Saisissez le chip-ID (se trouve sur l'emballage et à l'intérieur du cache de bouton).

**REMARQUE****Faible durée de vie des piles**

Lorsque Fast Wake-Up est activé, la serrure vérifie plus souvent si une action doit être effectuée. Cela réduit le temps de réaction mais conduit également à une diminution pouvant aller jusqu'à 30 % de la durée de vie des piles.

6. Activez Fast Wake-Up, en option.
7. Cliquez sur le bouton ENREGISTRER ou ENREGISTRER + COPIER.
 - ↳ ENREGISTRER enregistre la serrure et revient vers la matrice.
 - ↳ ENREGISTRER + COPIER enregistre la serrure et prépare dans le même temps une autre clé avec les mêmes propriétés.
- ↳ Serrure avec fonction en ligne (nœud de réseau) créée.

4.3 Supprimer la serrure avec des nœuds de réseau

Voici comment supprimer une serrure en ligne existante via le SmartBridge :

- ✓ SmartBridge créé (voir *Configurer les SmartBridges [► 19]*)
- ✓ Réseau créé et en état de fonctionnement
- ✓ Statut en ligne de la serrure à supprimer EN LIGNE.

1. Cliquez sur le Menu.
 - ↳ Le menu s'ouvre.
2. Cliquez sur le bouton RÉSEAU.
3. Dans le menu RÉSEAU, cliquez sur la serrure à supprimer.
4. Cliquez sur le bouton SUPPRIMER.
 - ↳ La suppression de la serrure sera alors signalisée.

5. Démarrez la configuration du réseau en cliquant sur le bouton DÉMARRER LA CONFIGURATION.
 - ↳ Étape de programmation (*dans ce cas la réinitialisation*) est effectuée.
 - ↳ La serrure peut ensuite être à nouveau reliée dans chaque installation de fermeture MobileKey.
- ↳ La serrure est supprimée.

4.4 Créer un clavier à PinCode en ligne

- ✓ Clavier PinCode en ligne déjà configuré (cf. Configuration).
 - ✓ Serrure pour clavier PinCode en ligne déjà configurée (cf. *Paramétrer la serrure avec des nœuds de réseau* [▶ 20]).
 - ✓ Aperçu de la matrice ouvert
1. Cliquez sur le symbole ajouter une clé (PLUS à côté du bouton SAVE).
 2. Choisir le type [CLAVIER PINCODE].
 3. Activez la Option VERSION EN LIGNE.
 4. Saisissez l'ID de la puce.
 5. Ouvrez le menu déroulant ▼ **Serrure**.
 6. Déterminez la serrure à laquelle le clavier PinCode en ligne sera utilisé.
 7. Donnez un nom pour un PIN, par ex. « Hans Müller ».
 8. Saisissez le PIN.
 9. Attribuez d'autres PIN de la même manière.



REMARQUE

Si vous souhaitez créer d'autres PIN utilisateur, vous devez alors cocher la case respective.



REMARQUE

Jusqu'à trois User-PIN peuvent être créés dans l'application Web MobileKey et être attribués à une serrure.

10. Cliquez sur le bouton **ENREGISTRER** ou **ENREGISTRER + COPIER**.
 - ↳ **ENREGISTRER** enregistre le clavier PinCode en ligne et revient ensuite à la matrice.
 - ↳ **ENREGISTRER + COPIER** enregistre le clavier PinCode en ligne et prépare immédiatement un nouveau clavier PinCode ayant les mêmes propriétés.
- ↳ Le clavier PinCode en ligne est créé.

**REMARQUE**

Si vous voulez ensuite éditer les User-PIN, veuillez alors cliquer sur l'entrée dans la matrice et sélectionner à partir du Menu, le bouton **MODIFIER**.

ATTENTION**Blocage après une mauvaise saisie**

Lorsqu'un mauvais User-PIN a été saisi sept fois, le SmartBridge consigne la réception mais le système bloque toutefois le traitement des User-PIN saisis pendant trois minutes. Un message respectif est affiché dans l'application Web.

Voir également sur ce point

➔ *Créer une serrure [▶ 9]*

4.5 Supprimer un clavier PinCode en ligne

- ✓ SmartBridge créé (cf. *Configurer les SmartBridges [▶ 19]*).
 - ✓ Réseau créé et en état de fonctionnement (cf. *Configurer les composants en ligne [▶ 24]*).
 - ✓ Statut en ligne du clavier PinCode en ligne à supprimer « EN LIGNE ».
1. Cliquez sur le Menu.
 - ↳ Le menu s'ouvre.
 2. Cliquez sur le bouton RÉSEAU.
 3. Dans le Menu « RÉSEAU » cliquez sur le clavier PinCode en ligne à supprimer.
 4. Cliquez sur le bouton SUPPRIMER.
 - ↳ Le clavier PinCode en ligne à supprimer est signalisé.
 5. Démarrez la configuration du réseau en cliquant sur le bouton **DÉMARRER LA CONFIGURATION**.
 - ↳ Étape de programmation (*dans ce cas la réinitialisation*) est effectuée.
 - ↳ Après avoir été préalablement réinitialisé à son état de livraison, le clavier PinCode en ligne (cf. Remise à l'état de livraison) peut ensuite être de nouveau raccordé à n'importe quelle installation de fermeture MobileKey.
- ↳ Le clavier PinCode en ligne a été supprimé.

4.6 Configurer les composants en ligne

- ✓ Au moins un SmartBridge créé.
 - ✓ SmartBridge relié à Internet et en état de fonctionnement
 - ✓ Au moins un serrure avec chip-ID en ligne créée
 - ✓ La distance entre le SmartBridge et les serrures doit être inférieure à 30 m. *Tous les composants doivent toujours se trouver dans le champ de radio du SmartBridge !*
1. Cliquez sur le Menu.
 - ↳ Le menu s'ouvre.
 2. Cliquez sur le bouton RÉSEAU.
 3. Cliquez sur le bouton DÉMARRER LA CONFIGURATION.
 - ↳ La configuration du réseau MobileKey s'effectue automatiquement.
- ↳ À l'issue de la configuration, les statuts des SmartBridges et des serrures doivent être sur EN LIGNE.

Veillez procéder aux vérifications suivantes si la configuration réseau automatique est restée sans succès : [Aide concernant les serrures en ligne \[▶ 38\]](#).

4.7 Programmation des composants

La programmation de serrures en ligne ou de claviers PinCode en ligne est également possible via SmartBridge. Les serrures ou transpondeurs doivent être programmé(e)s via un appareil de programmation USB car elles/ils n'ont pas de nœud de réseau (LockNode).



REMARQUE

Programmez chaque serrure ou clavier PinCode en ligne avant le montage !



REMARQUE

La liste des accès sauvegardée dans la serrure sera réinitialisée à chaque nouvelle programmation. Seuls les accès lus dans l'application Web seront conservés.

Voici comment effectuer une programmation via un SmartBridge :

- ✓ Saisir l'iD de puce de la serrure ou du clavier PinCode en ligne lors de la création
 - ✓ Réseau configuré avec succès
 - ✓ Aperçu de la matrice ouvert
1. Créer un composant.

2. Attribuez les autorisations, le cas échéant.
3. Cliquez sur « SAVE ».
 - ↳ La programmation démarre automatiquement via SmartBridge.
 - ↳ Pendant la programmation, le symbole de maintenance est affiché dans la matrice.

La programmation complète de la serrure est signalisée par un signal acoustique rapide, répété 3 fois. (*Bip, bip, bip*)

4.8 Couper la connexion des composants en ligne

Les composants en ligne peuvent si nécessaire être supprimés du système. Une suppression mécanique des composants (par ex. par le retrait du champ de portée radio de MobileKey) entraîne des alertes. C'est la raison pour laquelle, les composants doivent toujours être correctement déconnectés du système. La déconnexion entraîne la réinitialisation du nœud de réseau. La serrure ou le clavier PinCode en ligne conserve sa configuration et peut ensuite être contacté(e) à l'aide de la clé de programmation USB et ce, jusqu'à ce qu'une nouvelle configuration en ligne ait lieu.

- ✓ Au moins une serrure ou un clavier PinCode en ligne créé(e).
 - ✓ Au moins un SmartBridge créé.
1. Cliquez sur le Menu.
 - ↳ Le menu s'ouvre.
 2. Cliquez sur le bouton RÉSEAU.
 3. Cliquez sur la serrure à déconnecter ou sur le clavier PinCode en ligne à déconnecter.
 - ↳ Le menu s'ouvre.
 4. Dans le Menu, cliquez sur le bouton « DÉCONNECTER ».
 5. Démarrez la configuration en ligne en cliquant sur le bouton « DÉMARRER LA CONFIGURATION ».

Voir également sur ce point

➔ [Aide concernant les serrures en ligne \[► 38\]](#)

4.9 Effectuer une ouverture à distance

- ✓ Installation de fermeture correctement configuré
 - ✓ Accesspoint relié à Internet
 - ✓ La serrure dispose d'un nœud de réseau
 - ✓ La serrure est correctement configurée
 - ✓ Aperçu de la matrice ouvert
1. Cliquez sur la serrure que vous souhaitez ouvrir à distance.

2. Cliquez sur OUVRIR.
 - ↳ L'ordre est directement envoyé à la serrure via le SmartBridge. De cette manière, il est également possible de verrouiller une porte.
 - ↳ La serrure va être ouverte/fermée.

4.10 Key4Friends

Key4Friends permet de partager des clés via Smartphones. Les clés peuvent ainsi être facilement partagées avec des amis.

Votre ami reçoit un e-mail l'informant de la clé que vous lui avez partagée. L'e-mail décrit en détails comment cette clé peut être utilisée avec l'aide de l'application gratuite Key4Friends.

Votre ami installe l'application Key4Friends et s'enregistre rapidement et gratuitement à l'aide de son adresse e-mail et de son numéro de téléphone. Cette combinaison claire permet de garantir que votre clé ne puisse être utilisée que depuis le téléphone de votre ami.

4.10.1 Partager une clé

- ✓ Installation de fermeture correctement configuré
 - ✓ Accesspoint relié à Internet et en ligne
 - ✓ Aperçu de la matrice ouvert
1. Cliquez sur la serrure dont vous souhaitez partager la clé.
 - ↳ Le menu s'ouvre.
 2. Cliquez sur le bouton PARAMÉTRER KEY4FRIENDS.
 3. Saisissez les valeurs nécessaires.
 4. Complétez les informations relatives au destinataire.
 5. Limitez la validité de la clé.
 6. Cliquez sur le bouton ENVOYER.
- ↳ Votre ami reçoit immédiatement un e-mail. L'e-mail décrit précisément comment il peut utiliser la clé.

Tous les paramètres et informations concernant la clé partagée peuvent être modifiés ou supprimés à tout moment, voir Administrer clé [▶ 27].



REMARQUE

La fenêtre de temps pour les clés partagées est limitée à six mois.

- Si vous voulez donner un accès permanent à vos amis, utilisez des transpondeurs ou un Clavier PinCode.

4.10.2 Administrer clé






1. Cliquez sur le Menu.
 - ↳ Le menu s'ouvre.
2. Cliquez sur le bouton ADMINISTRER KEY4FRIENDS.
 - ↳ Sous le type Active, vous voyez toutes les clés actuellement partagées.
 - ↳ Sous le type Tous, vous voyez toutes les clés qui ne sont actuellement pas partagées.

Chaque clé partagée peut être modifiée ou supprimée par un clic.



4.11 Serrure DoorMonitoring - Affichage des états de la porte

Les serrures dotées de l'option DoorMonitoring communiquent les états de la porte à l'aide d'une vis de maintien spéciale. Ces serrures sont prévues pour MobileKey ONLINE et disposent donc d'un nœud de réseau de série.

Les états de porte suivants de la serrure DoorMonitoring sont affichés (parfois combinés) via un icône spécifique dans la matrice de l'application Web :

SYM-BOLE	DESCRIPTION
	Porte ouverte.
	Porte fermée mais pas verrouillée.
	Porte fermée de manière sûre et serrure verrouillée.
	Porte ouverte trop longtemps. <i>La durée peut être paramétrée dans les paramètres de la serrure seulement après la première programmation de la serrure DM</i>
	Porte fermée. État du verrouillage non surveillé.

La serrure DoorMonitoring peut, outre les alertes standard (*voir La matrice [▶ 7]*) afficher d'autres alertes :

SYM-BOLE	DESCRIPTION
Effraction	
	Une tentative d'effraction a été signalée au niveau de la porte. Il semblerait que la porte ait été forcée.
Manipulation de l'aimant	
	Quelqu'un a essayé de manipuler la porte et précisément la plaque magnétique.

Manipulation de la vis



Quelqu'un a essayé de manipuler la porte et précisément la vis de maintien.

Erreur du matériel



Des problèmes au niveau du capteur peuvent survenir mais ils sont très rares. Veuillez contacter votre revendeur spécialisé ou SimonsVoss Technologies GmbH (voir Aide & Contact) afin d'obtenir de l'aide. Il se pourrait que votre matériel doive être changé.



REMARQUE

Si une effraction ou une manipulation voulue de la serrure DoorMonitoring a été constatée, la porte concernée doit alors être immédiatement contrôlée. Veuillez vérifier qu'aucun dommage au niveau de la porte ou de la serrure ne soit présent. La serrure doit ensuite être réinitialisée ! Voir *Programmation des composants* [▶ 24]



ATTENTION

Pêne non surveillé

Lorsque le mode Flip-Flop est actif, l'état du pêne n'est pas surveillé !

- Renoncez au mode Flip-Flop si vous souhaitez également surveiller le pêne.



REMARQUE

La liste des accès sauvegardée dans la serrure sera réinitialisée à chaque nouvelle programmation. Seuls les accès lus dans l'application Web seront conservés.



REMARQUE

Veuillez noter que votre réseau MobileKey doit avoir été configuré avec succès ! Le statut du SmartBridge et de la serrure DoorMonitoring doit être sur EN LIGNE. Consulter *Aide concernant les serrures en ligne* [▶ 38] pour plus d'aide.


Voir également sur ce point

- ➔ *Aide concernant les serrures en ligne [▶ 38]*
- ➔ *Programmation des composants [▶ 24]*

5 Gestion des événements

Des messages ciblés peuvent être créés à l'aide de règles individuelles (événements). Ces messages peuvent non seulement être envoyés à différentes adresses e-mail mais aussi directement sur le Smartphone via des messages Push. Tous les messages seront en outre affichés sous MESSAGES dans l'application Web MobileKey.

5.1 Consulter les messages dans l'application Web

Tous les messages déclenchés via le gestionnaire d'évènements ainsi que toutes les informations importantes, alertes et alarmes sont affichés dans le Menu « MESSAGES » de la matrice (consultable via le symbole ).

Le symbole Messages du menu principal de la matrice permet de vous tenir informé de tous les derniers événements. Tous les événements peuvent être filtrés ou confirmés.

5.2 Créer des règles

Les événements individuels peuvent être créés dans les paramètres de l'installation de fermeture.

1. Cliquez sur le Menu.
↳ Le menu s'ouvre.
2. Cliquez sur le bouton REGLAGES.
3. Cliquez sur le bouton Plus sous GESTION DES ÉVÉNEMENTS.
↳ L'assistant à la création de nouvelles règles s'ouvre.

5.2.1 Créer une règle de type « Accès »

TYPE ACCÈS

DÉCLENCHEUR	DESCRIPTION
Ouverture à distance	Un message sera envoyé pour toutes les ouvertures à distance.
Key4Friends	Un message sera envoyé pour chaque et respectivement pour toutes les ouverture(s) déclenché(e)s via Key4Friends.
Transpondeurs /PIN	Un message sera envoyé pour chaque et respectivement pour toutes les ouverture(s) déclenchée(s) via une clé (transpondeur) ou un code PIN..

Cliquez sur SUIVANT après chaque étape. Lorsque tous les paramètres ont été fixés, vous pouvez activer l'évènement à l'aide du bouton ENREGISTRER.

1. Choisissez le type d'évènement ACCÈS.

2. Déterminez les clés qui doivent déclencher l'évènement.
 - ↳ Désactivez le curseur afin de limiter le nombre de clés et Key4Friends.
3. Déterminez les clés au moyen desquelles l'évènement doit être déclenché.
 - ↳ Désactivez le curseur afin de limiter le nombre de clés.
4. Déterminez la période à laquelle l'évènement doit être déclenché.
 - ↳ Toutes les durées sont sélectionnées par défaut afin que les évènements puissent être déclenchés à tout moment. Vous pouvez limiter les durées comme vous le souhaitez.
5. Saisissez un nom approprié pour l'évènement.
6. Saisissez la manière dont vous souhaitez être informé des évènements.
7. Cliquez sur le bouton ENREGISTRER.
 - ↳ L'évènement est désactivé.

5.2.2 Créer une règle de type « DoorMonitoring »

TYPE DOOR MONITORING

DÉCLENCHEUR	DESCRIPTION
Porte ouverte	Un message est envoyé dès que la porte est ouverte physiquement.
Porte fermée	Un message est envoyé dès que la porte est fermée physiquement.
Porte ouverte trop longtemps	Un message est envoyé dès que la porte est ouverte physiquement trop longtemps.
Porte fermée après ouverture trop longue	Un message est envoyé dès que la porte ouverte physiquement trop longtemps est refermée.
Porte déverrouillée	Un message est envoyé dès que la porte est déverrouillée.
Porte verrouillée	Un message est envoyé dès que la porte est correctement verrouillée.

Cliquez sur SUIVANT après chaque étape. Lorsque tous les paramètres ont été fixés, vous pouvez activer l'évènement à l'aide du bouton ENREGISTRER.

1. Choisissez le type d'évènement DOOR MONITORING.
2. Définissez les événements devant déclencher un évènement.
3. Déterminez les clés DoorMonitoring au moyen desquelles l'évènement doit être déclenché.
 - ↳ Désactivez le curseur afin de limiter le nombre de clés.

4. Déterminez la période à laquelle l'évènement doit être déclenché.
 - ↳ Toutes les durées sont sélectionnées par défaut afin que les évènements puissent être déclenchés à tout moment. Vous pouvez limiter les durées comme vous le souhaitez.
5. Saisissez un nom approprié pour l'évènement.
6. Saisissez la manière dont vous souhaitez être informé des évènements.
7. Cliquez sur le bouton ENREGISTRER.
 - ↳ L'évènement est désactivé.

5.2.3 Créer une règle de type « Alarme »

TYPE ALARME

DÉCLENCHEUR	DESCRIPTION
Pile faible	Un message est envoyé dès que l'état de chargement de la pile est faible.
Erreur de réseau	Un message est envoyé dès qu'il y a une erreur de réseau.
Effraction	Un message est envoyé dès qu'une serrure Door-Monitoring détecte une tentative d'effraction.
Problème de matériel	Un message est envoyé dès qu'un problème de matériel est détecté.

Cliquez sur SUIVANT après chaque étape. Lorsque tous les paramètres ont été fixés, vous pouvez activer l'évènement à l'aide du bouton ENREGISTRER.

1. Choisissez le type d'évènement ALARME.
2. Définissez les événements devant déclencher une alarme.
3. Saisissez un nom approprié pour l'évènement.
4. Saisissez la manière dont vous souhaitez être informé des évènements.
5. Cliquez sur le bouton ENREGISTRER.
 - ↳ L'évènement est désactivé.

5.3 Remarques importantes



REMARQUE

Tous les évènements sont transmis via le SmartBridge. Vous ne recevez aucun message lorsqu'il y a un problème au niveau de la connexion Internet ou de l'alimentation. Tous les évènements survenant pendant la durée durant laquelle le SmartBridge ne fonctionne pas correctement sont perdus.

**REMARQUE**

Un message de type « ALARME » est donc fortement recommandé. Voici comment paramétrer un tel évènement : *Créer une règle de type « Alarme »* [▶ 32]

**REMARQUE**

Les messages via évènements sont transmis en temps réel lorsque les serrures ont été mises en réseau avec le SmartBridge. Les alarmes des serrures non mises en réseau sont également saisies dès qu'une tâche de programmation est effectuée au niveau de la serrure respective. Sous « MESSAGES », vous pouvez afficher, filtrer et confirmer tous les évènements et alarmes.

Voir également sur ce point

➔ *Créer une règle de type « Alarme »* [▶ 32]

6 Aide

Les informations suivantes vous aideront à résoudre les problèmes quotidiens.

6.1 Aide avec des clés (transpondeurs)

La clé ou le transpondeur peuvent être perdus, endommagés ou volés. Tout cela oblige donc, dans le plan de fermeture, à supprimer l'ancienne clé et à créer une clé de remplacement. Pour des raisons de sécurité, toutes les autorisations de la clé supprimée doivent être retirées. Cela s'effectue au moyen d'une reprogrammation de toutes les serrures.

La procédure suivante décrit le remplacement d'une clé « non existante » ou défectueuse par une nouvelle clé.

✓ Aperçu de la matrice ouvert

1. Recherchez la clé concernée dans le plan de fermeture.
2. Supprimez toutes les autorisations.
3. Cliquez sur le bouton SAVE.
 - ↳ Les modifications sont sauvegardées.
4. Cliquez la clé dans le plan de fermeture.
 - ↳ Le menu s'ouvre.
5. Cliquez sur le bouton SUPPRIMER.
 - ↳ La réinitialisation de la serrure sera alors signalisée.
 - ↳ La tâche sera ensuite effectuée dans l'application de programmation.
6. En présence d'une clé perdue, volée ou défectueuse : Cliquez sur la clé concernée dans le plan de fermeture.
 - ↳ Le menu s'ouvre.
7. Cliquez sur le bouton FORCER LA SUPPRESSION.
 - ↳ La clé est supprimée du plan de fermeture.
 - ↳ La clé n'est pas encore bloquée dans le plan de fermeture.
8. Le cas échéant, créez une nouvelle clé.
9. Attribuez les autorisations nécessaires, le cas échéant.
10. Le cas échéant, cliquez sur le bouton ENREGISTRER ou ENREGISTRER + COPIER.
 - ↳ ENREGISTRER enregistre les clés et navigue avec la matrice.
 - ↳ ENREGISTRER + COPIER enregistre les clés et prépare dans le même temps d'autres clés avec les mêmes propriétés.
11. Cliquez sur le Menu.
 - ↳ Le menu s'ouvre.
12. Cliquez sur le bouton PROGRAMMER.
 - ↳ L'application de programmation démarre.

13. Exécutez toutes les tâches.

↳ Les tâches de programmation suivantes sont attendues : Retirer toutes les autorisations de la clé supprimée dans toutes les serrures et le cas échéant, autoriser une nouvelle clé aux serrures.

↳ La programmation va être effectuée.



ATTENTION

Accès non autorisé après un vol

Une clé volée reste autorisée dans l'installation de fermeture aussi longtemps que les autorisations n'ont pas été supprimées et que les serrures n'ont pas été reprogrammées !

- En cas de perte de clé, reprogrammer immédiatement toutes les serrures autorisées.

6.2 Aide avec serrures (par ex. cylindre de fermeture)

Les serrures ou cylindres de fermeture peuvent parfois être endommagé(e)s. Remplacez tout d'abord les piles de la serrure et essayez de la reprogrammer. Si la serrure ne fonctionne toujours pas, il faut alors la remplacer.

Si une serrure disposant d'autres propriétés est nécessaire, elle peut alors être tout simplement remplacée.

Veillez procéder de la manière suivante pour remplacer une serrure :

✓ Aperçu de la matrice ouvert

1. retirez la serrure concernée de la porte.

↳ *Il est parfois difficile de retirer une serrure d'une porte verrouillée. En cas de besoin, contactez le revendeur qui a installé vos produits SimonsVoss.*

2. Dans le plan de fermeture, cliquez sur la serrure à supprimer.

↳ Le menu s'ouvre.

3. Cliquez sur le bouton SUPPRIMER.

↳ La réinitialisation de la serrure sera alors signalisée.

↳ La tâche sera ensuite effectuée dans l'application de programmation.

4. En présence d'une serrure défectueuse : Cliquez sur la serrure.

↳ Le menu s'ouvre.

5. Cliquez sur le bouton FORCER LA SUPPRESSION.

↳ La serrure sera supprimée du plan de fermeture de manière irrévocable.

6. Créez une nouvelle clé.

7. Attribuez les autorisations nécessaires.
8. Cliquez sur le bouton ENREGISTRER ou ENREGISTRER + COPIER.
 - ↳ ENREGISTRER enregistre les clés et navigue avec la matrice.
 - ↳ ENREGISTRER + COPIER enregistre les clés et prépare dans le même temps d'autres clés avec les mêmes propriétés.
9. Créez une nouvelle serrure.
10. Attribuez les autorisations nécessaires.
11. Cliquez sur le bouton ENREGISTRER ou ENREGISTRER + COPIER.
 - ↳ ENREGISTRER enregistre les clés et navigue avec la matrice.
 - ↳ ENREGISTRER + COPIER enregistre les clés et prépare dans le même temps d'autres clés avec les mêmes propriétés.
12. Cliquez sur le Menu.
 - ↳ Le menu s'ouvre.
13. Cliquez sur le bouton PROGRAMMER.
 - ↳ L'application de programmation démarre.
14. Exécutez toutes les tâches.
 - ↳ La programmation va être effectuée.

6.3 Réinitialiser ou réutiliser les composants supprimés

Si un composant SimonsVoss (par ex. une clé ou serrure) a été supprimée de l'installation de fermeture, sans avoir été préalablement réinitialisé, il peut quand même être utilisé :

- ✓ Aperçu de la matrice ouvert
1. Créez les composants respectifs (par ex. clé ou transpondeur) dans le plan de fermeture.
 2. Cliquez sur le Menu.
 - ↳ Le menu s'ouvre.
 3. Cliquez sur le bouton PROGRAMMER.
 - ↳ L'application de programmation démarre.
 4. Exécutez toutes les tâches.
 - ↳ La première tentative de reprogrammation du composant fera apparaître un message d'erreur.
 5. Exécutez la tâche une nouvelle fois.
 - ↳ Le composant est à présent reprogrammé.

Veillez toujours correctement réinitialiser les composants afin d'éviter ce problème !

6.4 Lire les composants

Vous pouvez lire tous les composants MobileKey afin de savoir (ultérieurement) quelle est leur utilité. Cela peut par exemple être important lorsque vous trouvez une clé (par ex. un transpondeur) et que vous n'en connaissez pas l'utilisateur.

Les composants MobileKey peuvent être facilement lus :

1. Cliquez sur le Menu.
 - ↳ Le menu s'ouvre.
2. Cliquez sur le bouton **PROGRAMMER**.
 - ↳ L'application de programmation démarre.
3. Cliquez sur le bouton LIRE.



REMARQUE

Lecture sous macOS/Android

Au lieu de s'ouvrir dans l'application de programmation, l'interface de programmation s'ouvre dans la même application. Il n'y a pas de bouton LIRE. Au lieu de cela, cliquez sur le symbole de radio.

4. Sélectionnez les composants que vous souhaitez lire.
 - ↳ Le message affiche par ex. le nom de la clé (Hans Müller) ou s'il s'agit d'un composant MobileKey non programmé se trouvant à l'état par défaut.

6.5 Aide concernant SmartBridge

En présence d'un problème avec le SmartBridge, veuillez procéder aux vérifications suivantes si la configuration réseau automatique est restée sans succès :

- ❑ Vérifier l'**alimentation**.
 - ❑ La DEL du SmartBridge clignote-t-elle ?
- ❑ Vérifier la **connexion LAN**.
- ❑ Vérifier l'**accès Internet**.
 - ❑ Le Port 8883 (TCP/IP) du Firewall est-il ouvert ? Ajoutez, le cas échéant, les exceptions correspondantes afin que le SmartBridge puisse communiquer vers l'extérieur via le port 8883.
 - ❑ Le serveur DHCP est-il configuré de manière à ce qu'un appareil puisse s'inscrire dans le réseau ?

Via un ordinateur Windows, le SmartBridge peut également être commandé de manière optimale avec l'**outil OAM SimonsVoss**. L'outil OAM permet de régler les paramètres avancés du SmartBridge comme par exemple l'attribution d'une adresse IP fixe

ou les paramètres du server DHCP intégré. L'outil OAM se trouve sur la page d'accueil SimonsVoss (www.simons-voss.com) dans la section Assistance sous Téléchargements de logiciels.



REMARQUE

Utilisation d'adresses IP fixes

Lors de l'utilisation d'adresse IP fixe, le DNS (Domain Name Service) doit également être saisi via l'outil OAM.

- Vérifiez si les **Chip-ID et MobileKey-ID** ont été correctement saisis.
- La **distance** entre le SmartBridge et la serrure est-elle supérieure à 1,5 m et inférieure à env. 30 m ?
 - Testez le Setup et le cas échéant, la distance de 3 m (à vol d'oiseau) sans obstacle.
 - Les influences environnementales, les murs, objets et autres facteurs peuvent fortement influencer sur la qualité du signal. La couverture réseau jusqu'à 30 m ne peut pas être garantie.



REMARQUE

Réinitialiser le SmartBridge

Le SmartBridge peut être réinitialisé via une réinitialisation du matériel (cf. Réinitialiser le nœud de routeur).

6.6 Aide relative au clavier PinCode en ligne

Procédez aux vérifications suivantes en présence de problèmes avec le clavier PinCode en ligne.

- Vérifiez l'**état de la pile**. Procédez à un test de la pile (cf. Test des piles).
- Vérifiez que les **Chip-IDs** ont été correctement saisis.
- Vérifiez que la serrure ait été correctement attribuée au clavier PinCode en ligne (cf. *Créer un clavier à PinCode en ligne* [► 22]).

6.7 Aide concernant les serrures en ligne

En présence de **problèmes avec les serrures en ligne**, veuillez procéder aux vérifications suivantes si la configuration réseau automatique est restée sans succès :

- Vérifiez si les **Chip-ID** des serrures ont été correctement saisis.
- Vérifiez si les **nœuds de réseau ont été correctement montés**.

Lorsque le nœud de réseau et la serrure sont correctement en contact, 4 sons courts retentissent !

- Lors du montage ultérieur ou du remplacement des nœuds de réseau, vérifiez que les serrures ont été correctement attribuées !

6.8 Erreur de réseau

Vérifiez la stabilité de votre connexion Internet lorsque plusieurs erreurs de réseau surviennent dans les 24 heures.



REMARQUE

Nombreux sont les routeurs Internet qui changent d'adresse IP à certains intervalles de temps, ce qui peut donc parfois entraîner une coupure au niveau de la connexion Internet. Un message d'erreur peut apparaître (*la plupart du temps pendant la nuit*), lorsque cela dure plus de 30 secondes.

6.9 Réinitialisation manuelle des nœuds de réseau

Une serrure en ligne programmée se compose de deux composants séparément programmés : la serrure et le nœud de réseau. Les deux composants sont parfaitement appariés et ne peuvent, à l'état programmé, pas être utilisés dans une autre installation de fermeture. Réinitialisez toujours le nœud de réseau via l'application Web voir *Couper la connexion des composants en ligne* [▶ 25].

Si cette étape n'est pas possible, la configuration du nœud de réseau ne peut alors être réinitialisée qu'à l'aide d'une serrure n'appartenant pas à l'installation de fermeture. Pour ce faire, montez le nœud de réseau sur une fermeture inconnue. La réinitialisation du nœud de réseau sera signalisée après quelques secondes :

- Cylindre de fermeture : Signal acoustique (4x bip)
- SmartRelais : signal optique par DEL. (Veillez à ce que l'alimentation soit correcte !)

À l'issue de la réinitialisation, le nœud de réseau peut être relié à n'importe quel SmartBridge.

7 Maintenance, nettoyage et désinfection



Dompage causé aux surfaces

L'utilisation d'un détergent ou d'un désinfectant inapproprié ou agressif peut endommager les composants MobileKey.

Ne pas laisser les composants MobileKey au contact d'huile, de peintures, de graisses ou d'acides !

Lors de la désinfection, il convient d'utiliser des produits expressément prévus pour la désinfection des surfaces métalliques ou matières plastiques délicates.



ATTENTION

Remplacement des piles

Les piles vides doivent être remplacées par de nouvelles piles préconisées par SimonsVoss. Les anciennes piles doivent toujours être jetées en respectant la réglementation en vigueur !

8 Applications MobileKey

L'application MobileKey est disponible dans les App-Stores iOS et Android. Cette application supporte les fonctions suivantes :

- Aperçu des états des portes (lors de l'utilisation de cylindres DM).
- Ouvertures à distance.
- Envoi d'autorisations Key4Friends.
- Lecture et affichage des listes des accès.
- Réception des messages Push du gestionnaire d'évènements.
- Utilisation de Touch-ID pour les actions sécurisées (ouverture à distance, Key4Friends, désactivation des messages Push).
- Programmation de clé et serrures via une clé de programmation USB.
Disponible seulement pour les appareils Android avec fonction OTG et câble OTG supplémentaire.

9 Déclaration de conformité

Les documents tels que les déclarations de conformité et autres certificats peuvent être consultés en ligne sous www.simons-voss.com.

10 Conseils & Astuces

10.1 Raccourci vers l'application Web

Il est possible de créer un raccourci vers l'application Web MobileKey sur chaque appareil. Cela permet ainsi de démarrer rapidement et facilement l'application Web sur le bureau de votre ordinateur mais aussi depuis un Smartphone ou une tablette. À vous d'essayer !

10.2 Utilisation de clés sans clé de programmation USB

À l'heure actuelle, toutes les clés (transpondeurs) doivent être programmées à l'aide de la clé de programmation USB. Cela est particulièrement difficile en l'absence d'accès à un appareil Windows ou Android. L'exemple ci-après vous montre comment attribuer une clé préprogrammée à l'aide d'un terminal supporté sans clé de programmation USB :

- ✓ Serrure avec extension EN LIGNE
 - ✓ Serrure avec le statut EN LIGNE
 - ✓ Aperçu de la matrice ouvert
1. Créez tout d'abord plusieurs clés par ex. « Extra1, Extra2, Extra3, etc. ».
 - ↳ Ces clés ne disposent tout d'abord d'aucune autorisation.
 2. Programmez toutes les clés à l'aide de la clé de programmation USB et marquez-les avec le nom respectif (optionnel).
 - ↳ Une lecture de la clé est bien entendu également possible ultérieurement.
 3. Au lieu de devoir créer une nouvelle clé et de la programmer à l'aide d'une clé de programmation US, modifiez simplement les paramètres d'une clé précédemment créée par ex. « Extra1 ».
 4. Cliquez sur la clé déjà créée par ex. « Extra1 » et sélectionnez MODIFIER.
 5. Modifiez le nom.
 6. Saisissez, si vous le souhaitez, les données pour Valable à partir de et Valable jusqu'à.
 7. Cliquez sur le bouton ENREGISTRER et retournez à la matrice.
 - ↳ La clé est enregistrée.
 8. Autorisez la clé aux serrures souhaitées.
 9. Cliquez sur le bouton SAVE.
 - ↳ L'aperçu de la matrice s'ouvre.
 10. Cliquez sur la serrure à laquelle la clé doit être autorisée.
 - ↳ Le menu s'ouvre.
 11. Cliquez sur le bouton
 12. Cliquez sur le bouton **PROGRAMMER**.
 - ↳ La programmation a lieu en ligne via le SmartBridge.

13. Répétez cette étape jusqu'à ce que vous ayez programmé toutes les serrures.

↳ Les clés sont autorisées aux serrures sélectionnées.

10.3 Paramétrer la langue

Vous pouvez paramétrer la langue de l'application Web en toute simplicité. Sont disponibles :

- Anglais
- Danois
- Allemand
- Français
- Italien
- Néerlandais
- Suédois

Procédure à suivre :

- ✓ Aperçu de la matrice ouvert
- 1. Cliquez sur le symbole Menu
 - ↳ Le Menu de la page de droit s'ouvre.
- 2. Cliquez sur la saisie portant votre nom.
 - ↳ Le menu change.
- 3. Cliquez sur le bouton COMPTE.
 - ↳ Le menu Données du compte s'affiche.
- 4. Cliquez sur le bouton LANGUES.
 - ↳ Le menu déroulant pour les langues s'affiche.
- 5. Sélectionnez votre langue.
 - ↳ La langue est paramétrée.

11 Aide et autres informations

Documentation/documents

Les informations détaillées concernant le fonctionnement et la configuration peuvent être consultées sur la page d'accueil de SimonsVoss dans la section téléchargements sous documentation (<https://www.simons-voss.com/fr/telechargements/documents.html>).

Logiciels et pilotes

Les logiciels et pilotes se trouvent sur la page d'accueil de SimonsVoss dans la section téléchargements sous téléchargement de logiciels (<https://www.simons-voss.com/fr/telechargements/telechargements-de-logiciels.html>).

Déclarations de conformité

Les déclarations de conformité relatives à ce produit peuvent être consultées sur la page d'accueil SimonsVoss, dans la section certificats (<https://www.simons-voss.com/fr/certificats.html>).

Informations sur l'élimination

- Ne jetez pas l'appareil (MobileKey) avec vos ordures ménagères mais dans un point de collecte communal pour appareils électriques et appareils spéciaux conformément à la directive européenne 2012/19/UE.
- Recyclez les piles défectueuses ou usées conformément à la directive européenne 2006/66/CE.
- Veuillez tenir compte des dispositions locales applicables concernant la collecte séparée des piles.
- Recyclez l'emballage d'une manière écologique.



Hotline

En cas de questions techniques, contactez la Hotline SimonsVoss au +49 (0) 89 99 228 333 (appel vers le réseau fixe allemand, coût variable en fonction de l'opérateur).

E-Mail

Vous préférez nous envoyer un e-mail ?

support@simons-voss.com

FAQ

Les informations et aides relatives aux produits SimonsVoss peuvent être consultées sur la page d'accueil de SimonsVoss dans la section Section FAQ (<https://faq.simons-voss.com/otrs/public.pl>).

SimonsVoss Technologies GmbH
Feringastrasse 4
85774 Unterföhring
Allemagne



Voici SimonsVoss

SimonsVoss est le leader de la technologie en matière de systèmes de fermeture numérique.

Le pionnier de la technique de fermeture fonctionnant par radio et sans câblage proposant des solutions de systèmes avec une large gamme de produits pour les domaines SOHO, moyennes et grandes entreprises ainsi que pour les établissements publics.

Les systèmes de fermeture SimonsVoss allient fonctionnalité intelligente, qualité sans compro-

mis et design primé « Made in Germany ». En tant que fournisseur de systèmes innovant, SimonsVoss attache une grande importance à l'adaptabilité des systèmes, à la sécurité maximale, à la fiabilité des composants, à la performance des logiciels et à la simplicité d'utilisation.

L'esprit d'innovation, la durabilité, la responsabilité et la haute estime des collaborateurs et partenaires constituent les principes de la réussite économique.

L'entreprise ayant son siège social à Unterföhring près de Munich et un site de production à Osterfeld (Saxe-Anhalt) emploie plus de 300 collaborateurs dans huit pays.

SimonsVoss est une société du Groupe ALLEGION – un réseau actif à l'échelle mondiale dans le domaine de la sécurité. Allegion est représenté dans près de 130 pays (www.allegion.com).

© 2019, SimonsVoss Technologies GmbH, Unterföhring

Tous droits réservés. Les textes, photos et graphiques sont protégés par les droits d'auteur.

Le contenu de ce document ne peut être copié, diffusé ou modifié. Sous réserve de modifications techniques.

SimonsVoss et MobileKey sont des marques enregistrées de la société SimonsVoss Technologies GmbH.

