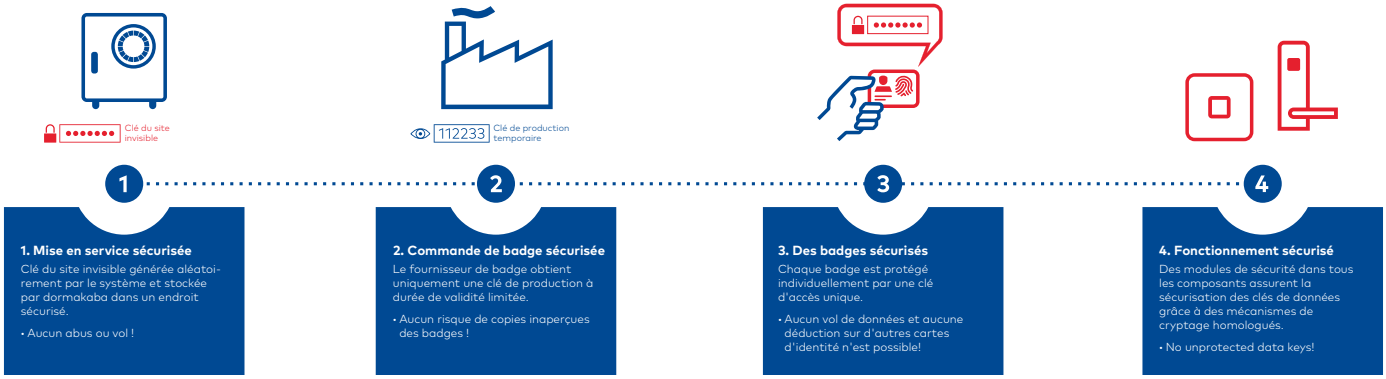
Livre blanc : concept de sécurité dormakaba ARIOS-2

Pourquoi ARIOS-2 vous offre plus de sécurité pour MIFARE®



MIFARE est une technologie RFID largement répandue. Avec le concept de sécurité ARIOS-2, dormakaba, en tant que fournisseur de solutions complètes, propose des mécanismes supplémentaires et sophistiqués par rapport aux solutions MIFARE courantes, qui rendent votre contrôle d'accès encore plus sécurisé.

Un élément central d'ARIOS-2 est la clé de sécurité unique, qui est générée par un générateur aléatoire et n'est visible pour personne. Cela permet d'assurer un haut niveau de sécurité à toutes les étapes du procédé : de la génération, à la mise en service, en passant par la production de badges, jusqu'à la maintenance. Par exemple, lors de la commande de badges, un code spécifique est créé pour chaque installation pour le fabricant de badges. Ce n'est que lorsque les nouveaux badges seront livrés que ce code sera converti en clé du site via un processus ARIOS-2 sécurisé et ce processus sera consigné dans le système afin que les badges produits illégalement ne puissent pas être utilisés de manière inaperçue.

De plus, l'échange de données entre le lecteur et le badge est crypté au moyen de procédures AES ou 3DES homologuées. Cela protège les opérateurs de système contre les scénarios d'attaque actuels courants tels que les procédés d'ingénierie inverse ou les attaques de l'homme du milieu. Les mécanismes de sécurité ARIOS-2 s'étendent même aux badges individuels. Cela signifie que le cryptage des données est individuel pour chaque badge. Les attaquants n'ont ainsi également aucune chance de tirer des conclusions sur le chiffrement d'une installation globale.

ARIOS-2 de quoi s'agit-il ?

Le concept de sécurité ARIOS-2 comble une lacune de sécurité dans les applications RFID, dont le mécanisme de sécurité est basé sur une clé de données personnalisée par l'utilisateur.

Sans ARIOS-2, la clé de données MIFARE peut facilement être transmise ou espionnée. Le concept de sécurité ARIOS-2 aide les utilisateurs à stocker leurs clés de données en toute sécurité et facilement, de sorte que le transfert ou la manipulation inaperçus sont empêchés et le niveau de sécurité du système est augmenté.
Ce document explique les différents mécanismes de sécurité et les éléments fondamentaux du concept de sécurité et indique clairement les gains de sécurité que les utilisateurs obtiennent avec ARIOS-2 pour leur solution de contrôle d'accès.

dormakaba

dormakaba ARIOS-2 – concept de sécurité

Les éléments centraux

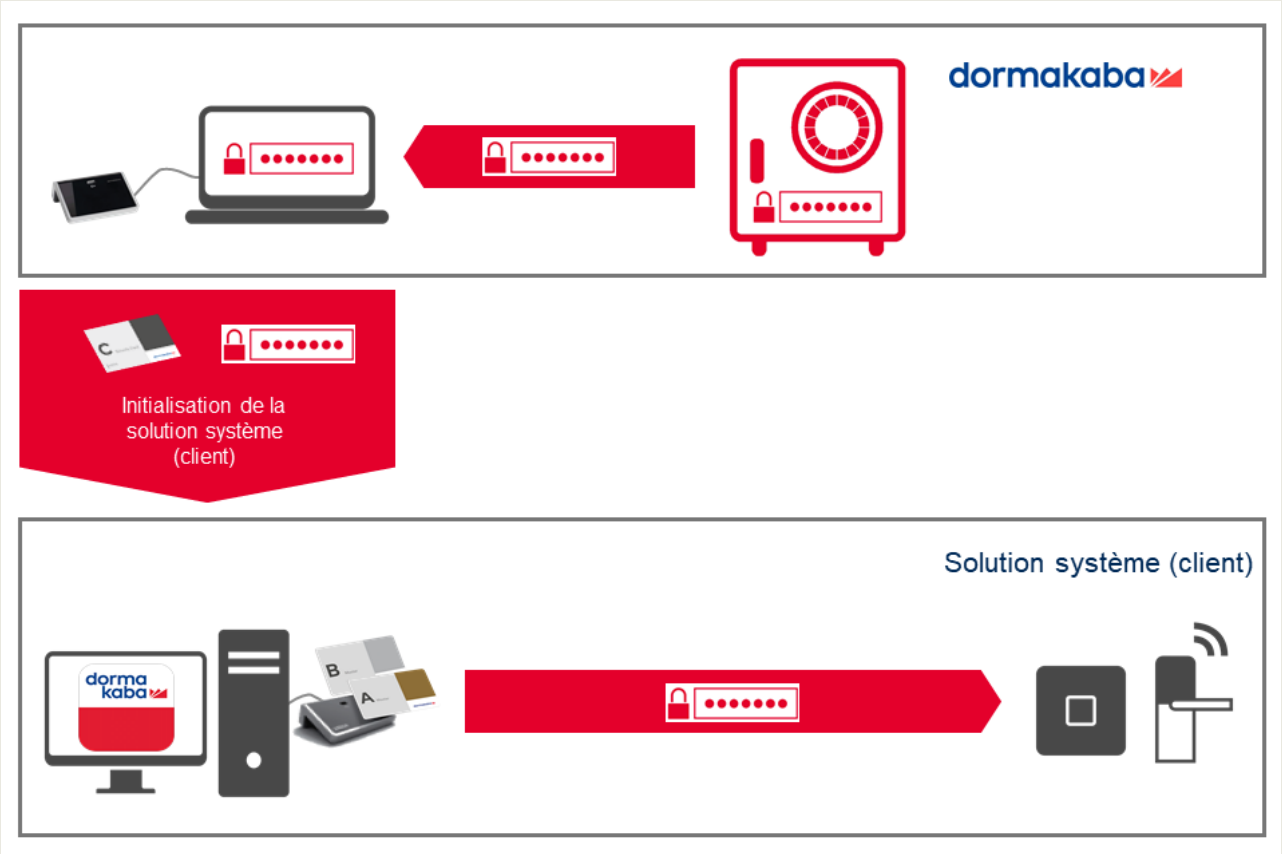
1. Clé du site

L'élément central du concept de sécurité ARIOS-2 est la clé du site. Le concept ARIOS-2 assure que la clé du site reste toujours inconnue. La clé secrète et invisible du site spécifique au client est générée dans un environnement dormakaba particulièrement sécurisé par dormakaba et conservée en toute sécurité.

Avec ARIOS-2, différentes installations peuvent être exploitées indépendamment les unes des autres grâce à la clé du site.

ARIOS-2 offre une sécurité supplémentaire dans la mesure où la clé du site n'est pas utilisée pour l'autorisation directe d'un média utilisateur, comme cela est habituellement le cas avec les applications MIFARE. La clé du site dans ARIOS-2 sert de base au calcul de la clé d'accès individuelle à un média utilisateur.

La clé du site et les médias d'autorisation – jamais visibles, ni lisibles



2. Médias d'autorisation (médias Master)

Après avoir été générée, la clé du site sera apportée sur l'installation via un média d'autorisation. Les médias d'autorisation permettent au propriétaire de mettre l'installation en service et d'apporter des modifications. Le grand avantage d'un tel média d'autorisation est qu'il peut être utilisé de manière contrôlée à tout moment et qu'une divulgation orale et écrite est empêchée. Le concept est basé sur la « propriété » et non sur la « connaissance » (secret partagé).

Deux types de médias d'autorisation sont employés dans le concept de sécurité ARIOS-2 :
- Carte de sécurité (type C)
- Programme principal (type A/type B)

2.1. Carte de sécurité C

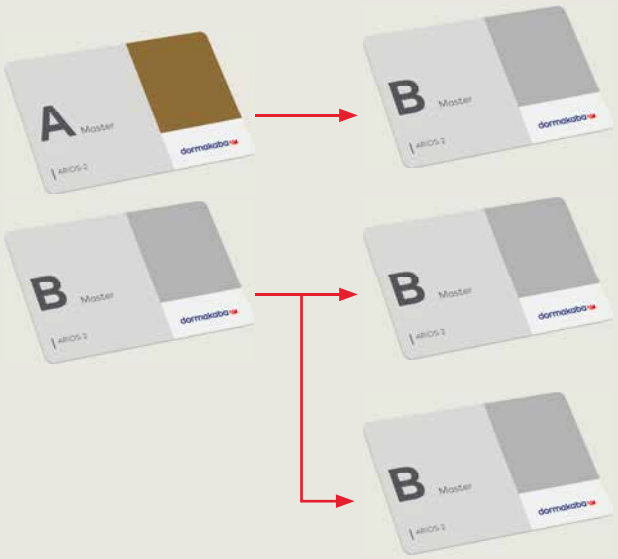
La carte de sécurité C est un badge RFID permettant d'initialiser l'application système et doit donc être conservée en lieu sûr après utilisation. La carte de sécurité C est fournie par dormakaba, elle est de type MIFARE DESFire. Les données essentielles pour la sécurité telles que la clé du site et les données de configuration sont conservées sous forme cryptée sur la carte de sécurité C (3DES ou AES). Le lecteur de table dormakaba est nécessaire pour utiliser la carte de sécurité C. Lors de la mise en service, la clé du site cryptée avec 3DES ou AES est transférée de la carte de sécurité ou du programme principal vers tous les composants du système et stockée. La clé du site n'est visible à aucun moment. Le transfert vers des composants standalone est effectué manuellement (sur site) avec le programme principal. Vers les composants online via l'infrastructure du système (central).

2.2. Programme principal A/B

Les programmes principaux sont des cartes d'identité RFID avec lesquelles les composants standalone sont initialisés, pris en charge et programmés. Pour des raisons administratives, les contenus peuvent être transmis à d'autres programmes principaux (pas de doubles). Les programmes principaux sont fournis par dormakaba, ils sont de type MIFARE DESFire. Les données relatives à la sécurité telles que la clé du site sont stockées sous forme chiffrée sur le programme principal (3DES ou AES). Le lecteur de table dormakaba est requis pour l'utilisation.

Carte de sécurité C

Programme principal A et B



Médias d'autorisation dans l'aperçu

	Cartes de sécurité	Master de programmation
Types	Type C	Type A/Type B
Fonctions	Initialisation des applications système (disponible au moins une fois par installation)	initialisation de composants standalone
Peut créer des copies	Non	Non (transmission possible que de manière limitée)
Média	MIFARE DESFire (sans contact)	MIFARE DESFire (sans contact)
Contenu des données	– Copie chiffrée des données de sécurité ARIOS-2 – Données de configuration de l'installation	Copie chiffrée des données de sécurité ARIOS-2

3. Puce de sécurité dans le lecteur de table

Le lecteur de table 91 08 MRD est un composant important lors de la configuration de la solution d'accès. Lors de la configuration, la carte de sécurité C doit être placée sur le lecteur de table et lue. Si l'application système ou l'ordinateur du poste de travail est éteint, les données de sécurité contenues dans le lecteur de table seront perdues.

Les applications système disposant de leur propre autorisation utilisateur (par exemple Kaba exos 9300) peuvent également stocker les données de sécurité sur la carte de sécurité dans la base de données spécifique au système.

Après le démarrage du lecteur de table initialisé, les données de sécurité sont rechargées. Cela signifie que la carte de sécurité ne doit être présentée qu'une seule fois lors de la mise en service du lecteur de table, car les données de sécurité sont également chiffrées dans l'application système (3DES). Cette fonction de confort assure un fonctionnement efficace sans failles de sécurité. Si le lecteur de table est volé (déconnecté de l'application système), il perd toutes les données. En fonctionnement normal, ce lecteur de table est utilisé pour émettre et lire des médias.

dormakaba ARIOS-2
Mécanismes d'accès et de chiffrement

La génération automatique de la clé du site assure qu'elle reste toujours secrète. Dans le cas peu probable où la clé du site d'une quelconque installation serait piratée, seule cette installation serait compromise en raison de la structure d'autorisation horizontale et il ne serait pas possible de tirer des conclusions sur une autre installation. La sécurité serait rétablie en générant une nouvelle clé du site pour cette installation. Le chiffrement 3DES ou AES128 est utilisé pour répartir la clé du site au sein d'une installation et pour l'accès aux médias utilisateur. Les mécanismes de chiffrement utilisés peuvent être mis à la disposition des opérateurs du système intéressés à tout moment.

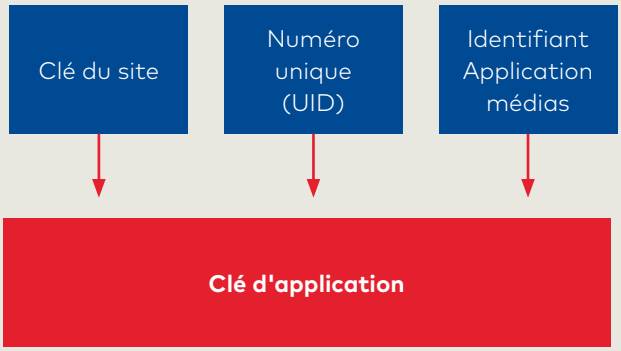
Clé du site
La clé du site est générée par un générateur aléatoire certifié.

Clé d'application
La clé d'application est utilisée pour accéder (authentification) aux données sur le média utilisateur. Pour des raisons de sécurité, chaque application possède sa propre clé d'application sur chaque média utilisateur.

Cette méthode assure un niveau de sécurité élevé. S'il était possible de déchiffrer une clé d'application, seule cette application sur ce média utilisateur serait compromise. Il ne serait pas possible de tirer des conclusions sur les autres médias utilisateur.

Le codage de la clé d'application est le suivant :
- Clé du site de l'application
- Numéro unique du média utilisateur
- Identifiant de l'application média respective

Composition de la clé d'application



Clé de lecture de médias
Cette clé permet à un système tiers ou à un appareil tiers qui ne prend pas en charge le concept ARIOS-2 de lire le numéro d'identification programmé sur le média utilisateur. En plus de cette clé de lecture des médias, d'autres données structurelles sont transmises à l'exploitant afin que le numéro puisse être lu et interprété correctement.

Clé d'application tierce
La clé d'application tierce assure la migration pendant le fonctionnement. Pour continuer à utiliser les médias utilisateur tiers existants, ARIOS-2 prend en charge l'application concrète suivante :

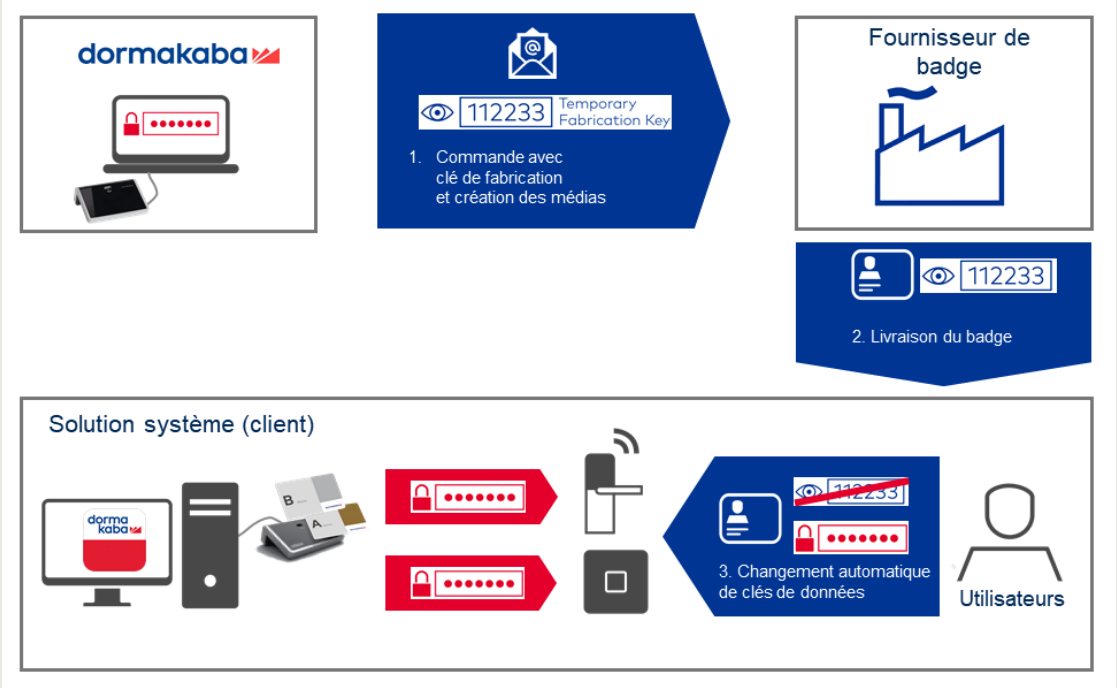
- Lecture du numéro d'identification d'une application tierce.
  Dans ce cas, les médias d'autorisation ARIOS-2 de l'installation sont étendus avec l'application tierce. La clé d'application tierce occupe le même espace mémoire qu'une clé du site.

L'application concrète suivante est également possible pour la migration des badges tiers existants sans clé d'application tierce :

- Lire le numéro d'identification
  Pour lire le numéro d'identification ARIOS-2, l'application ARIOS-2 doit être copiée sur les médias utilisateur.

Clé de fabrication
La création de médias utilisateur représente un défi en matière de sécurité dans le monde MIFARE. Habituellement, une définition (types de badge) des médias utilisateur souhaités et de la clé secrète est transmise au fabricant de la carte. Cela signifie que l'on fait confiance au fabricant de la carte, un contrôle n'est pas possible. La clé de fabrication comble cette lacune. Parce qu'elle est dérivée de la clé du site, la clé de fabrication est générée pour chaque fichier (Classic) ou application (DESFire) et ne peut pas être recalculée. La clé de fabrication est remise au fabricant avec la commande de production. Si le média utilisateur est ensuite utilisé pour la première fois sur l'application système, celle-ci reconnaît la clé de fabrication et l'échange avec la clé d'application du média utilisateur, qui est unique pour chaque média utilisateur et chaque fichier/application. Si un fabricant de médias produisait deux fois la même identification, celle-ci serait reconnue et tous les médias portant cet ID seraient immédiatement bloqués.

Création et initialisation des médias sécurisés à l'aide d'une clé de fabrication



Avez-vous des questions ? Nous serons ravis de vous accueillir et de vous conseiller.

dormakaba Belgium N.V. | Monnikenwerve 17-19 | BE-8000 Brugge | T +32 50 45 15 70 | info.be@dormakaba.com | www.dormakaba.be
dormakaba France S.A.S. | 2-4 rue des Sarrazins | FR-94046 Créteil cedex | T +33 1 41 94 24 00 | marketing.fr@dormakaba.com | www.dormakaba.fr
dormakaba Luxembourg SA | Duchscherstrooss 50 | LU-6868 Wecker | T +352 26710870 | info.lu@dormakaba.com | www.dormakaba.lu
dormakaba Suisse SA | Chemin de Budron A5 | CH-1052 Le Mont-sur-Lausanne | T +41 848 85 86 87 | info.ch@dormakaba.com | www.dormakaba.ch