dormakaba ARIOS-2

FAQ : Réponses aux questions les plus importantes

1. Introduction

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 connue de l'opérateur du système. Avec ARIOS-2, les attaquants n'ont aucune chance de tirer des conclusions sur le chiffrement d'une installation globale.

Ce document offre des réponses aux questions les plus importantes concernant la technologie MIFARE utilisée par dormakaba en employant ARIOS-2.
Ce document ne décrit pas les détails du concept ARIOS-2. Ceci est documenté sous la forme du papier blanc ARIOS 2, servant de base à la compréhension de ce document. Aucune question spécifique concernant la technologie MIFARE n'est traitée ci-dessous. Veuillez vous référer pour cela aux publications MIFARE : http://www.mifare.net/

2. Stratégie

2.1 Pourquoi dormakaba-t-elle propose des solutions 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 système d'accès encore plus sécurisé.

3. Technologie et compatibilité

3.1 Quelles sont les différences entre les systèmes qui fonctionnent avec MIFARE Standard, MIFARE avec ARIOS-2 et LEGIC ?

Arguments	LEGIC	ARIOS-2	MIFARE Standard
Gestion des clés	hiérarchique à plusieurs niveaux	à un niveau	aucun(e)
Clé	Jeton physique	Jeton physique	Connaissance
Carte Master (primaire)	Carte RFID standard de LEGIC (avec Clé hiérarchique) ; Condition requise : Partenaire de licence	aucun(e)	aucun(e)
Carte Master (secondaire)	Carte RFID standard (LEGIC) du fournisseur du système	Standard (MIFARE DESFire) Carte RFID de dormakaba (sans clé)	aucun(e)
Générer une carte Master	Détenteur d'une licence	dormakaba	aucun(e)
Gestion des applications	un fichier de définition par application et une ou plusieurs cartes Master (IAM)	toutes les applications dans une carte Master	en fonction du fournisseur de système
Applications tierces (capacité multi-applications)	peut être complété par une définition propre et une carte Master sur les mêmes médias utilisateur	indépendant d'ARIOS-2 sur les mêmes médias utilisateur (médias ouverts pour d'autres applications)	selon le fournisseur de système
Générer des clés	mécanisme de transmission fixe basé sur le secret	génération masquée (aléatoire) dans le matériel	définition libre ouverte/ visible
Enregistrement des clés	Carte Master et matériel de lecteur	Zone protégée chez dormakaba, Carte Master et Matériel de lecteur	Papier ou fichier local, Matériel de lecteur
Répartir des clés	manuellement via la carte Master avec protection R/W ; sinon assuré via le chipset du lecteur	automatiquement via l'infrastructure système (transport sécurisé)	manuellement via le logiciel de configuration
Accès par carte via l'interface RF	L'accès au média peut être limité par des procédures de lancement (lecteurs). Advant : ouvert ou DES/3DES, où la clé est prédéfinie et secrète Prime : processus propriétaire	Classique : processus propriétaire (Crypto 1) DESFire : 3DES / AES128 clés individuelles par carte et par application/fichier	Classique : processus propriétaire (Crypto 1) DESFire : 3DES / AES128 / AES256

3.2 Puis-je utiliser des composants tiers dans les solutions système ?
Si l'interface d'intégration de ce composant tiers prend en charge nos solutions et que le composant permet la programmation d'une clé d'application externe, elle peut être utilisée pour la lecture. Nous recommandons de ne pas utiliser ces composants dans des configurations essentielles pour la sécurité, par exemple utilisation uniquement à l'intérieur. Pour rendre cela possible, ARIOS-2 propose une « clé en lecture seule » dans le cadre du concept. La licence du concept ARIOS-2 n'est pas prévue pour des tiers.

3.3 Puis-je utiliser une carte MIFARE dormakaba avec d'autres systèmes ?
MIFARE DESFire : Oui, à condition qu'il y ait suffisamment d'espace mémoire et que la clé principale PICC soit disponible.
MIFARE Classic : Oui, à condition d'utiliser l'UID, le MAD ou un secteur libre.

3.4 Puis-je utiliser une structure de données MIFARE d'un fournisseur tiers avec des systèmes dormakaba ?
Oui, si la « clé en lecture seule » du client est connue et qu'il existe un numéro de badge unique.

3.5 Puis-je étendre un système dormakaba installé avec ARIOS-2 ?
Une extension est possible. Cependant, les composants existants ne seront pas dotés du concept de sécurité ARIOS-2. En fonctionnement parallèle, l'application ARIOS-2 doit être copiée sur la structure de données existante sur le média utilisateur.

Si le concept de sécurité dormakaba est nécessaire, les modifications suivantes s'imposent :
- Le matériel existant doit être remplacé s'il ne prend pas en charge le concept de sécurité ARIOS-2.
- Le logiciel doit être mis à jour.
- Les médias doivent être dotés d'une structure de données supplémentaire. Cela se fait généralement avec une solution de kiosque. Pour cela il doit y avoir suffisamment de mémoire médias libre disponible.

Dans le cas d'installations de fournisseurs tiers, les ajustements nécessaires doivent être clarifiés en fonction du projet !

3.6 Puis-je utiliser des applications tierces avec ARIOS-2, par exemple pour les cantines ou pour des systèmes tiers.
Non, car le codage est limité aux applications ARIOS-2. Pour cela il faut utiliser un système tiers.

3.7 Quels médias sont en règle générale pris en charge par les différentes solutions ?
Pour des informations plus détaillées, veuillez vous référer au tableau suivant.

Tableau pour 3.7 Quels médias sont en règle générale pris en charge par les différentes solutions ?

	LEGIC	ARIOS-2	MIFARE Standard
Technologies RFID prises en charge	LEGIC advant : ISO 14443 A ISO 15693 LEGIC prime : LEGIC RF	MIFARE Classic 1k, 4k MIFARE DESFire 8k (standard), 4k, 2k ISO 14443 A (UID uniquement) d'autres sont possibles	MIFARE Classic MIFARE DESFire
Acquisition de médias	du détenteur d'une licence LEGIC	tout fabricant de cartes	tout fabricant de cartes
Programmation des médias	configuration libre selon les règles LEGIC (recommandation du concédant de licence) ; plusieurs normes pour une compatibilité indépendante des fabricants	Choix de définitions propriétaires fixes (assurant la compatibilité entre les systèmes compatibles ARIOS-2, coordonnés avec les fournisseurs de médias. Par conséquent, manipulation facile, seulement un minimum de savoir-faire est nécessaire)	configuration libre dans le cadre des règles MIFARE, telles que définies par le fournisseur du système ; pas de normes
Moyen pour la programmation des médias	SW : LEGIC CSW ou propres outils du licencié + HW spécial	Outil de programmation (recommandation : UniC10)	selon le fournisseur de système
Autorisation pour la programmation de médias	Carte Master spécifique à l'installation physiquement nécessaire pour la station de programmation de la carte	Fichier avec clé de fabrication individuelle (connaissances) ; pas identique à la clé du site.	Clé du site (connaissances) ou solution dépendante du fournisseur du système
Sécurité organisationnelle :	basée sur la « propriété » **advant** : Sécurisé d'un point de vue technique (aucune faille de sécurité publiée) **prime** : Sécurité limitée d'un point de vue technique (failles de sécurité connues publiées)	basée sur la « propriété » **DESFire** : Sécurisé d'un point de vue technique (aucune faille de sécurité publiée) **Classic** : Sécurité limitée d'un point de vue technique (failles de sécurité connues publiées)	basée sur la « connaissance » (généralement plus important pour la sécurité) **DESFire** : Sécurisé d'un point de vue technique (aucune faille de sécurité publiée) **Classic** : Sécurité limitée (failles de sécurité connues publiées)

3.8 Les cartes Classic et DESFire peuvent-elles être utilisées en parallèle dans un seul système ?

Oui.
Pour des raisons de sécurité, l'utilisation de médias DESFire est recommandée. En outre, le Traceback des médias n'est pris en charge qu'avec des médias DESFire.
Conditions requises générales :

- Mémoire suffisante disponible sur le média existant
- Code d'accès (écriture/lecture) disponible pour carte.

Une solution de kiosque est un appareil qui fournit l'application ARIOS-2 aux cartes existantes.
Cet appareil est installé chez le client.

Tableau pour 3.8 : Utilisation parallèle de différentes technologies MIFARE

Situation initiale	Passer à MIFARE Classic ARIOS-2	Passer à MIFARE DESFire ARIOS-2
MIFARE Classic	**Carte existante** 1. Codage supplémentaire 2. Solution de kiosque nécessaire 3. Changer le matériel du lecteur **Changer de carte pendant le fonctionnement** 1. Changer le matériel du lecteur 2. Mettre de nouvelles cartes en place	**Changer de carte pendant le fonctionnement** 1. Changer le matériel du lecteur 2. Mettre en place de nouvelles cartes utilisateur
MIFARE Classic ARIOS-2		**Changer de carte pendant le fonctionnement** Fonctionnement mixte en fonction du système et de la configuration 1. Nouvelle carte Master 2. Mettre en place de nouvelles cartes utilisateur
MIFARE DESFire		**Carte existante** Fonctionnement mixte en fonction du système et de la configuration. 1. Codage supplémentaire 2. Solution de kiosque nécessaire 3. Changer le matériel du lecteur **Changer de carte pendant le fonctionnement** Fonctionnement mixte en fonction du système et de la configuration. 1. Changer le matériel du lecteur 2. Mettre en place de nouvelles cartes utilisateur

4. Sécurité

4.1 Une carte MIFARE Classic peut-elle être copiée ou modifiée à l'identique ?
Comme on le sait, le code de sécurité de la carte MIFARE Classic a été déchiffré. Cependant, cela ne signifie pas que les cartes MIFARE Classic avec ARIOS-2 ne sont pas sûres. Pour effectuer une manipulation, les connaissances, méthodes et outils nécessaires pour réaliser un piratage MIFARE doivent être connus, d'une part, et il doit y avoir un accès à un lecteur dans une installation, d'autre part, dans le but de collecter des données sur l'établissement de la connexion et de déterminer la clé d'application

Cependant, les composants ARIOS-2 ont des mécanismes qui compliquent la tâche grâce à :
- Un délai d'authentification,
- Un délai dû à un circuit de réveil pour les composants standalone,
- Une utilisation de différentes clés.

4.2 Comment fonctionne le concept de sécurité ?
Essentiellement, le concept de sécurité est basé sur une mémoire clé sécurisée, dans laquelle toutes les clés sont conservées comme dans un coffre-fort. Il n'est pas possible d'accéder directement de l'extérieur à ces clés. Cette mémoire clé est contenue dans une carte de sécurité (clé du site) et dans chaque composant de l'installation tels que les lecteurs, les composants standalone, etc. Le concept de sécurité ARIOS-2 est détaillé dans le papier blanc ARIOS-2.

4.3 En quoi le concept de sécurité ARIOS-2 diffère-t-il de la concurrence ?
ARIOS-2 est un concept de sécurité dormakaba qui, d'une part, est indépendant de la technologie RFID sélectionnée et, d'autre part, offre des mécanismes de protection supplémentaires à la technologie RFID utilisée.

Qui sont :
1. Mise en service sécurisée
   Clé du site invisible générée aléatoirement par le système et conservée par dormakaba dans un endroit sécurisé.
   --> Aucun abus ou vol !
2. Commande de badge sécurisée
   Le fournisseur de badge obtient uniquement une clé de production temporaire. Conversion en clé du site invisible lors de la première utilisation.
   --> Aucun risque de copies inaperçues des badges !
3. Des badges sécurisés
   Chaque badge individuel est sécurisé par une clé d'accès unique.
   --> Aucun vol de données et aucune déduction possible par rapport à d'autres badges !
4. Fonctionnement sécurisé
   Les modules de sécurité de tous les composants sécurisent les clés de données à l'aide de mécanismes de chiffrement homologués.
   --> Aucune clé de données non protégée !

Tableau pour 4.1 : Comparaison de la sécurité des installations

	MIFARE Classic Standard	MIFARE Classic ARIOS-2
Toutes les cartes ont la même clé d'application.	Cela correspond à l'application concrète la plus courante. Les médias peuvent être copiés sans gros obstacles.	non utilisé
Chaque carte a sa propre clé d'application.	Il existe des fournisseurs d'appareils MIFARE qui disposent d'une protection supplémentaire, similaire à ARIOS-2. Cela signifie qu'une seule carte peut être copiée. La sécurité dépend de l'application.	Avec ARIOS-2, chaque média a sa propre clé (Application Key). La sécurité est en outre renforcée par le fait que la clé d'application dépend de l'UID de la carte utilisateur.

4.4 Quelles applications médias sont basées sur le concept de sécurité ARIOS-2 ?
Les données d'accès sont stockées dans une structure de données similaire à celle de LEGIC. Le tableau ci-dessous compare les segments LEGIC connus.

4.5 Comment ARIOS-2 assure sa protection contre les différents types d'attaque ?
Les mécanismes sont décrits aux chap. 4.2 et 4.3. De plus amples informations sont disponibles dans le papier blanc ARIOS-2.

4.6 Quel est le degré de sécurité du fonctionnement UID ?
La norme ISO 14443A n'assure aucune sécurité lors du fonctionnement UID. Dans le cas d'ARIOS-2, une méthode « Save UID » est prise en charge. Avec cette méthode, un paquet de données (KCA) [2] est lu à partir du média en plus de l'UID. L'autorisation d'accès est désormais déterminée à l'aide d'une procédure cryptée. Si un UID sans KCA est à présent simulé, le code d'accès ne peut pas être déterminé.

4.7 Une clé doit-elle être remise au fabricant de la carte ?
Une clé de fabrication est remise au fabricant de la carte. Cette clé est utilisée uniquement pour la production de cartes. Si une carte est intégrée à l'installation, la clé de fabrication est remplacée par la clé d'application. Ce processus est vérifié et enregistré par le système. De cette manière, tout double généré par le fabricant de la carte est reconnu, puisque cette conversion de la clé ne peut être effectuée qu'une seule fois pour une carte utilisateur ayant le même UID.

Tableau pour 4.4 : Structure des données dormakaba ARIOS-2

Configuration

Segments LEGIC	**Fichier MIFARE Classic ARIOS-2**	**Applications MIFARE DESFire ARIOS-2**
Kaba Group Header	Fichier d'identification	Application Access
CardLink	Données CardLink État de l'actionneur CardLink	Données CardLink État de l'actionneur CardLink Traceback
LockerLock Sélection libre	LockerLock Sélection libre	LockerLock Sélection libre
Biométrie		Application biométrique

Le segment cash, par exemple, n'est pas inclus, car ces applications sont fournies par des fournisseurs tiers.

5. Médias MIFARE

5.1 Quels médias utilisateur peuvent être utilisés ?
Il est recommandé d'utiliser des médias utilisateur du même type dans l'installation. Les fabricants peuvent varier. La distance de lecture peut varier en fonction du fabricant, car les processus de production ne sont pas standardisés. Dans le cas MIFARE, nous vous recommandons d'utiliser uniquement des cartes de fabricants « certifiées MIFARE ».

5.2 Qui peut coder des cartes ?
Chaque fabricant de cartes peut coder des cartes en utilisant la clé de fabrication.

5.3 Où peut-on obtenir la carte ?
En principe, les médias utilisateur peuvent être obtenus auprès de n'importe quel fournisseur de cartes ou auprès de dormakaba. dormakaba fournit uniquement des médias avec la technologie MIFARE DESFire recommandée.
Les cartes de sécurité et les programmes principaux sont exclusivement fournis par dormakaba.

5.4 Puis-je changer de fournisseur de cartes après la première livraison ?
Oui.

En cas de changement, les informations suivantes doivent être fournies au fabricant de la carte :
- Fichier AEF (format XML) ou Print Information (format PDF), créé avec Media-Workstation (MWS)

5.5 Une carte MIFARE Classic ou DESFire existante peut-elle être utilisée ?
Oui, la clé de maintenance des médias doit être connue en tant que condition préalable.

Nous distinguons deux cas :
1. L'application ARIOS-2 doit être copiée (terminal) sur le média existant. Pour cela , il faut qu'il y ait suffisamment d'espace libre sur le média.
2. Le numéro programmé existant doit être lisible. Pour cela, le codage du numéro doit être connu.

Les détails à ce sujet doivent être clarifiés avec les spécialistes ARIOS-2.

Tableau pour 5.1 : Quels médias utilisateur peuvent être utilisés avec ARIOS-2 ?

Type de carte	Taille de mémoire [2]	Applications système prises en charge
MIFARE DESFire EV1/EV2	8 ko recommandés 2 ko et 4 ko possibles	CardLink (KXA) Protégé par UID (KCA)
MIFARE Classic	1 ko, 4 ko	CardLink Protégé par UID (KCA)

[2] Des cartes de différentes tailles de mémoire peuvent être utilisées dans une installation.