FAQ
dormakaba ARIOS-2 Security Concept

Enhanced security for MIFARE® applications:
Answers to the most important questions.

dormakaba

1. Introduction

The ARIOS-2 security concept closes a security gap in RFID applications that have security mechanism based on a data key that is known to the system operator. With ARIOS-2, attackers do not have an opportunity to draw conclusions about the encryption of an entire system.

This document provides ARIOS-2 users with answers to the most important questions regarding the MIFARE® technology used by dormakaba.

However, this document does not describe the ARIOS-2 concept in detail. This is documented in the ARIOS-2 white paper, which serves as the basis for understanding this document.
It also does not answer any specific questions regarding MIFARE® technology. For this purpose, we refer you to the MIFARE® publications: https://www.mifare.net/

2. Strategy

2.1 Why does dormakaba offer MIFARE® solutions?
MIFARE® is a widely-used RFID technology. With the ARIOS-2 security concept, as a complete solution provider, dormakaba offers additional mechanisms that make your access control system even more secure compared to common MIFARE® solutions.

3. Technology and compatibility

3.1 What is the difference between systems operated with MIFARE® Standard, MIFARE® with ARIOS-2 and LEGIC?

Arguments	LEGIC	MIFARE® with ARIOS-2	MIFARE® Standard
Key management	Multi-stage hierarchical	Single-stage	No
Key	Physical token	Physical token	Knowledge
Primary master card	RFID card from LEGIC (incl. hierarchical key); prerequisite: licence partners	None	None
Secondary master card	LEGIC RFID card from the system supplier	MIFARE® DESFire® RFID card from dormakaba (without key)	None
Creation of master card	Licensee	dormakaba	No
Application management	One definition file and one or more master cards (IAM) per application	All applications in a master card	Dependent on system supplier
Third-party applications (multi-application capability)	Option of expansion on the same user media by means of its own definition and master card	Independent of ARIOS-2 on the same user media (media open to other applications)	Dependent on system supplier
Key generation	Fixed inheritance mechanism based on secret	Hidden (random) generation in hardware	Free open/visible definition
Key storage	Master card and reader hardware	Protected area at dormakaba, master card and reader hardware	Paper or local file, reader hardware
Key distribution	Manually via master card with R/W protection; otherwise secured via reader chipset	Automatically via system infrastructure (protected transport)	Manually via configuration software
Card access via RF interface	LEGIC prime: proprietary procedure LEGIC advant: 3DES, key cannot be changed and is secret. Access to the medium can be restricted within the launch procedure (reader).	MIFARE Classic®: proprietary procedure (Crypto 1) MIFARE® DESFire®: 3DES/AES-128 Individual keys per card and application	MIFARE Classic®: proprietary procedure (Crypto 1) MIFARE® DESFire®: 3DES/AES-128

3.2 Can I use third-party components in the system solutions?

If the integration interface of this third-party component supports our solutions and the component allows programming of a third-party application key, it can be used in a readable manner. We recommend that you do not use such components in security-relevant configurations, e.g. interior use only. To make this possible, ARIOS-2 offers a "read only key" as part of the concept. There are no plans to license the ARIOS-2 concept for third parties.

3.3 Can I use a dormakaba MIFARE® card with other systems?

- MIFARE® DESFire®: Yes, provided there is sufficient memory and the PICC master key is made available.
- MIFARE Classic®: Yes, if the (Unique IDentification number), MAD (MIFARE® Appliation Directory) or a free sector is used.

3.4 Can I use a third-party MIFARE® data structure with dormakaba systems?
Yes, if the customer's "Read only key" is known and a unique ID number exists.

3.5 Can I extend an installed dormakaba system with ARIOS-2?
Extension is possible. However, the existing components will not have the ARIOS-2 security concept. In the case of parallel operation, the ARIOS-2 application must be applied to the user medium in addition to the existing data structure.

If the dormakaba security concept is required, the following changes are necessary:

- Existing hardware must be replaced if it does not support the ARIOS-2 security concept.
- The software must be updated.
- Media must be provided with an additional data structure. This is usually done with a kiosk solution. To do this, you must have enough free media memory.

In the case of third-party systems, the necessary adaptation must be clarified on a project-specific basis!

3.6 Can I link third-party applications e.g. for cafeterias or **external systems with ARIOS-2?**
No, the encoding is limited to ARIOS-2 applications. A third-party system must be used for this purpose.

3.7 What media are supported in principle by the different solutions?
For more information, see the following table.

Table for 3.7 What media are supported in principle by the different solutions?

	LEGIC	MIFARE® with ARIOS-2	MIFARE® Standard
Supported RFID technologies	LEGIC advant: ISO 14443 A ISO 15693 LEGIC prime: LEGIC RF	MIFARE® DESFire® MIFARE Classic® ISO 14443 A	MIFARE® DESFire® MIFARE Classic® ISO 14443 A
Media relation	By LEGIC licensee	Any card manufacturer	Any card manufacturer
Media programming	Free configuration within the LEGIC rules (licensor recommends); some standards for manufacturer independent compatibility	Choice of fixed proprietary definitions (Ensuring compatibility between ARIOS-2 compatible systems, coordinated with media suppliers. As a result, simple operation and only minimal level of expertise required)	Free configuration within the MIFARE® rules, according to the system provider definition; no standards
Media programming tools	SW: LEGIC CSW or licensee's own tools + specific HW	Programming tool (Recommended: UniC10)	Dependent on system supplier
Authorization for media programming	System-specific master card at card programming station physically necessary	File with individual fabrication key (knowledge); not identical to site key.	Site key (knowledge) or solution dependent on system supplier
Organisational security:	based on "ownership" LEGIC advant**:** Technically secure (no published security gaps) LEGIC prime: Technically unsafe (known published security gaps)	based on "ownership" MIFARE® DESFire®: Technically secure (no published security gaps) MIFARE Classic®: Technically unsafe (known published security gaps)	based on "knowledge" (usually security-critical) MIFARE® DESFire®: Technically secure (no published security gaps) MIFARE Classic®: Limited security (known published security gaps)

3.8 Can MIFARE Classic® and MIFARE® DESFire® cards be used in parallel in one system?

Yes.
For security reasons, the use of MIFARE® DESFire® media is recommended. In addition, support for media tracebacks is only available with DESFire media.
General requirements:

- Sufficient memory available on the existing medium
- Access code (write/read) for map available

A kiosk solution is a device that the ARIOS-2 application superimposes on existing cards. This device is installed at the customer's premises.

Table for 3.8: Parallel use of different MIFARE® technologies

Initial situation	Switch to MIFARE Classic® with ARIOS-2	Switch to MIFARE® DESFire® with ARIOS-2
MIFARE Classic®	**Existing cards** 1. Additional coding 2. Kiosk solution necessary 3. Exchange reader hardware Card exchange during operation 1. Exchange reader hardware 2. Roll out new cards	**Card exchange during operation** 1. Exchange reader hardware 2. Roll out new user cards
MIFARE Classic® with ARIOS-2		**Card exchange during operation** Mixed operation depending on system and configuration 1. New master card 2. Roll out new user cards
MIFARE® DESFire®		**Existing cards** Mixed operation depending on system and configuration. 1. Additional coding 2. Kiosk solution necessary 3. Exchange reader hardware **Card exchange during operation** Mixed operation depending on system and configuration. 1. Exchange reader hardware 2. Roll out new user cards

4. Security

4.1 Can a MIFARE Classic® card be copied or modified?

As you know, the security code of the MIFARE Classic® card was decrypted. However, this does not mean that MIFARE Classic® cards with ARIOS-2 are insecure. In order to carry out a manipulation, on the one hand, the knowledge, methods and tools for the MIFARE® hack must be known and, on the other hand, there must be access to a reader in a system in order to collect data about the connection set-up and determine the application key

However, the ARIOS-2 components have mechanisms that make this more difficult due to:

- Delayed authentication
- Delay due to wake-up switching on standalone components
- Use of different keys

4.2 How does the security concept work?

The security concept is essentially based on a secure key store in which all keys are stored as if in a safe. From the outside, it is not possible to access those keys directly. This key store is contained in a security card (site key) and in each system component such as readers, standalone components and so on. More details about the ARIOS-2 security concept can be found in the ARIOS-2 white paper.

4.3 How does the ARIOS-2 security concept differ from its competitors?

ARIOS-2 is a dormakaba security concept, which, on the one hand, exists independently of the selected RFID technology and, on the other, offers additional protection mechanisms for the RFID technology used.

Those are the following:

- Safe commissioning
  Concealed site key, randomly generated by the system, which is stored by dormakaba in a protected location.
  → No misuse or theft

- Secure ID card ordering
  The ID card supplier only receives a temporary production key. Conversion to concealed site key on first use.
  → No undetected ID card copies

- Secure ID cards
  Each ID card is individually protected by a unique access key.
  → No data theft and no conclusions about other ID cards possible

- Secure operation
  Security modules in all components protect the data keys by recognised encryption mechanisms.
  → No unprotected data keys

4.4 Which media applications are based on the ARIOS-2 security concept?

Access data is stored in a data structure similar to LEGIC. The table below shows a comparison with the known LEGIC segments.

4.5 How does ARIOS-2 protect itself against different types of attacks?

The mechanisms are described in chapters 4.2 and 4.3. Further information can be found in the ARIOS-2 white paper.

4.6 How secure is a UID operation?

The ISO 14443A standard does not provide security during UID operation. In the case of ARIOS-2, a save UID method is supported. In addition to the UID, this method reads a data key from the medium. An encrypted procedure then determines the access permission. If a UID is simulated without data key, the access code cannot be determined.

4.7 Does a key have to be submitted to the card manufacturer?

A fabrication key is submitted to the card manufacturer. This key is used only for the production of cards. If a card is integrated into the system, the fabrication key is replaced by the application key. This process is checked and logged by the system. This will detect any duplicate created by the card manufacturer, as this key conversion can only be done once for a user card with the same UID.

Table for 4.4: dormakaba ARIOS-2 data structure

Configuration

Segment Description	MIFARE Classic® with ARIOS-2 file	MIFARE® DESFire® with ARIOS-2 applications
Identification	Identification	Identification
CardLink	CardLink	CardLink
Actuator Status	Actuator Status	Actuator Status
TraceBack	n/a	TraceBack
Free selection	n/a	Free selection

Remark: Cash Segment is not included because these applications are supplied by third parties.

5. MIFARE® media

5.1 Which user media can be used?
It is recommended to utilise user media of the same type in the system.

5.2 Who can encode cards?
Any card manufacturer can encode cards with the production key.

5.3 Where can I get the cards?
In principle, the user media can be obtained from any card supplier or from dormakaba. dormakaba supplies media with MIFARE® DESFire® technology. The security cards and programming masters are supplied exclusively by dormakaba.

5.4 Can I change the card supplier after the initial delivery?
Yes. In the event of a change, the following information must be provided to the card manufacturer:

- DCD file (XML format) or print information (PDF format) created with Media Work Station (MWS)

5.5 Can an existing MIFARE Classic® or MIFARE® DESFire® card be used?
Yes, but the media maintenance key must be known as a basic requirement:

- The ARIOS-2 application must be brought onto the existing medium. To do this, there must be enough free memory space on the medium.
- Details can be clarified with the ARIOS-2 specialists.

dormakaba ARIOS-2 depends on the dormakaba access solution used.

Subject to technical changes without prior notice.

Any questions? We will be happy to assist you.

dormakaba International Holding AG | Hofwisenstrasse 24 | CH-8153 Rümlang | info.de@dormakaba.com | dormakaba.com