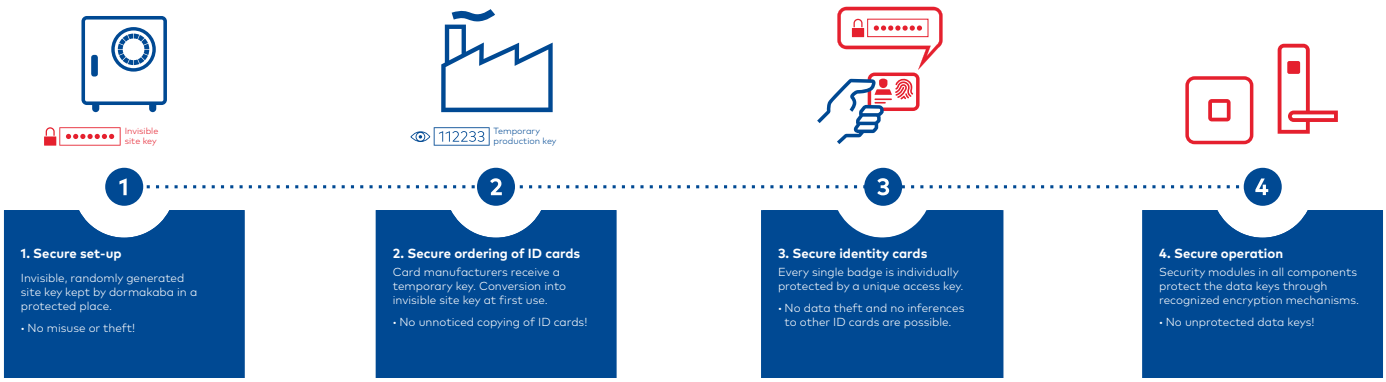
White paper: dormakaba ARIOS-2 security concept

Why ARIOS-2 provides you with increased security for MIFARE®



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

A central element of ARIOS-2 is the unique security key, which is generated by a random generator and not visible to anyone. This provides a high level of security for all process steps: from generation, commissioning, ID card production to maintenance. For example, for ID card orders, a specific code is created per system for the ID card manufacturer. Only when the new ID cards are delivered is this code converted into the site key using a secure ARIOS-2 process. This process is logged in the system and means that no illegally produced ID cards can be used undetected.

In addition, the data exchange between the reader and the ID card is encrypted using the recognised AES or 3DES procedures. This protects system operators against current common attack scenarios such as the so-called reverse engineering process or man-in-the-middle attack. The ARIOS-2 security mechanisms even extend to the individual ID card. This means that the data encryption is specific to each ID card. Attackers therefore would not have an opportunity to draw conclusions about the encryption of an entire system.

What is ARIOS-2?

The ARIOS-2 security concept closes a security gap in RFID applications that have a security mechanism based on a user-defined data key.

Without ARIOS-2, the MIFARE data key can easily be passed on or spied on undetected. The ARIOS-2 security concept supports users with the easy and secure storage of their data key, preventing unnoticed disclosure or manipulation and increasing the system security level.
This document explains the individual security mechanisms and core elements of the security concept and shows users how ARIOS-2 enhances the security of their access control solution.

dormakaba

dormakaba ARIOS-2 – Security concept
Core elements

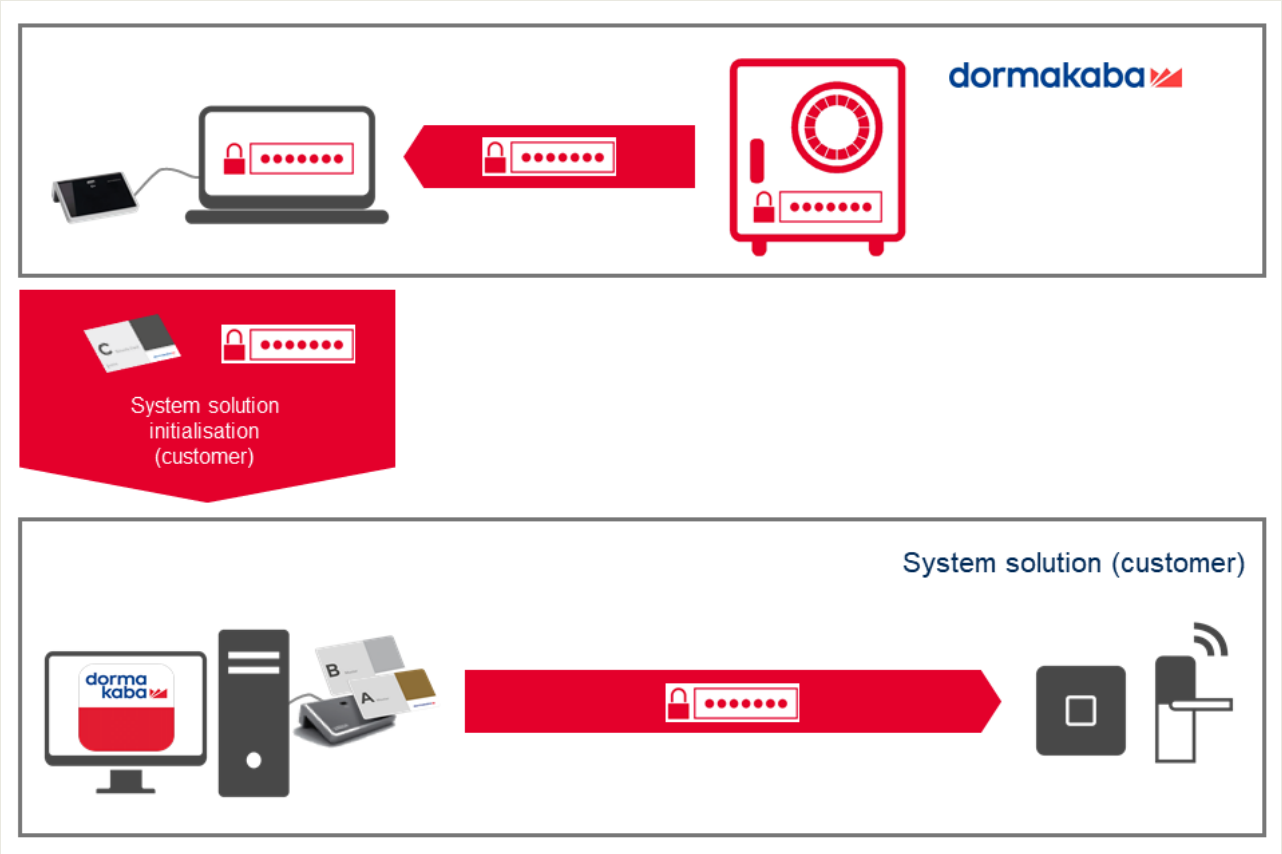
1. Site key

The central element of the ARIOS-2 security concept is the site key. The ARIOS-2 concept ensures that the site key is not known at any time. The customer-specific, secret and concealed site key is generated by dormakaba in a specially protected environment and stored securely.

With ARIOS-2, different systems can be operated completely independently of each other thanks to the site key.

ARIOS-2 provides additional security by not using the site key for the direct authorization of a user medium, as is usually the case in MIFARE applications. In ARIOS-2, the site key provides the calculation basis for calculating the individual key for accessing a user medium.

Site keys and authorization media – never visible and readable



2. Authorization media (master media)

The site key is conveyed to the system after an authorization medium is generated. The authorization media allow the owner to put the system into operation and to make changes. The great advantage of this kind of authorization medium is that it can be used at any time in a controlled manner. Verbal and written disclosure is prevented. The concept is thus based on "ownership" rather than "knowledge" (shared secret).

The ARIOS-2 security concept uses two types of authorization media:

- Security card (type C)
- Programming masters (type A/type B)

2.1. Security card C

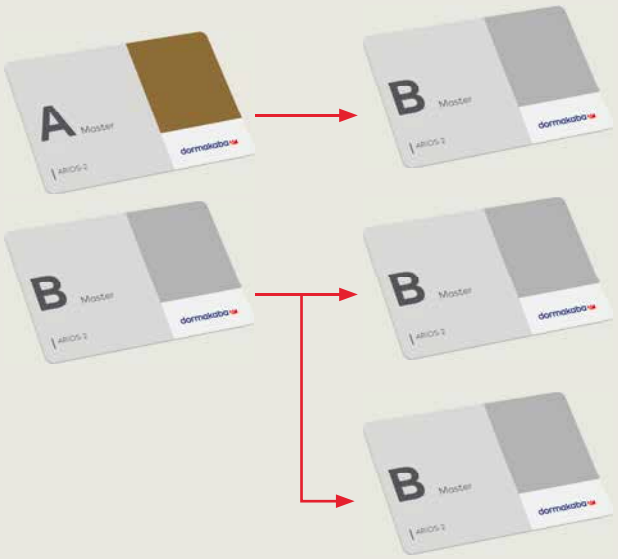
The security card C is an RFID card for initialising the system application and should therefore be stored in a safe place after use. The security card C, which is of MIFARE DESFire type, is provided by dormakaba. Security-relevant data such as the site key and configuration data are stored on the security card C in encrypted form (3DES or AES). To use the security card C, the dormakaba desktop reader is required. During commissioning, the site key, which is encrypted with 3DES or AES, is transferred from the security card or programming master to all system components and stored there. The site key is not visible at any time. On standalone components, the transfer is carried out manually (on-site) with the programming master. On online components, it is carried out via the system infrastructure (centrally).

2.2. Programming masters A/B

Programming masters are RFID cards used to initialise, maintain and program standalone components. For administrative reasons, the contents can be passed on to other programming masters (no duplicates). The programming masters, which are of MIFARE DESFire type, are provided by dormakaba. Security-relevant data such as the site key are stored on the programming masters in encrypted form (3DES or AES). The dormakaba desktop reader is required to use these.

Security card C

Programming master A and B



Overview of authorization media

	Security cards	Programming master
Types	Type C	Type A/Type B
Functions	Initialising system applications (available at least once per system)	Initialising standalone components
Can create copies	No	No (optional limited heredity transmission)
Medium	MIFARE DESFire (contactless)	MIFARE DESFire (contactless)
Data content	– Encrypted copy of ARIOS-2 security data – System configuration data	Encrypted copy of ARIOS-2 security data

3. Security chip in desktop reader

The desktop reader 91 08 MRD is an important component in the configuration of the access solution. During configuration, the security card C must be placed on the table reader and read. If the system application or workstation is switched off, this security data in the desktop reader is lost.

System applications with their own user authorization (e.g. Kaba exos 9300) can also store the security data of the security card in the native database.

After starting the initialised desktop reader, the security data is reloaded. The security card therefore only has to be placed once during commissioning of this desktop reader because the security data is also encrypted in the system application (3DES). This convenient function enables efficient working without security gaps. If the desktop reader is stolen (disconnected from the system application), it loses all data. In normal operation, this desktop reader is used to output and read media.

dormakaba ARIOS-2
Access and encryption mechanisms

The automatic generation of the site key ensures that it is not known at any time. In the unlikely event that the site key of any system is hacked, the flat authorization structure means that only this one system would be compromised and conclusions about another system would not be possible. Security would be restored by generating a new site key for this system. 3DES or AES128 encryption is used to distribute the site key within a system and for access to user media. The encryption mechanisms used may be made available to interested system operators at any time.

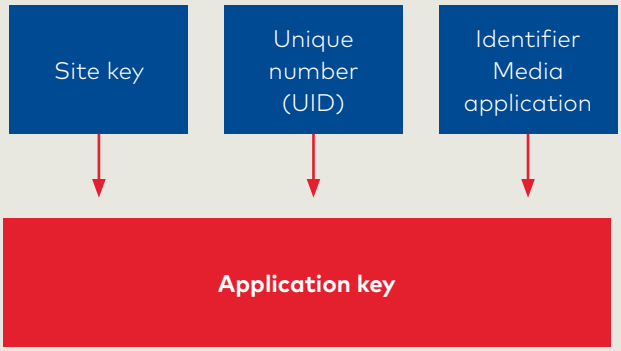
Site key
The site key is generated using a certified random generator.

Application key
The application key provides access (authentication) to the data in the user medium. For security reasons, each application has its own application key on each user medium.

This method achieves a high level of security. If someone manages to decrypt an application key, only this application is endangered on this user medium. Conclusions about other user media are not possible.

The application key in the encoding consists of the following:
- Site key of the application
- Unique number of the user medium
- Identifier of the respective media application

Composition of application key



Media read key
This key allows a third-party system or a third-party device that does not support the ARIOS-2 concept to read the programmed identification number on the user medium. In addition to this media read key, additional structural data is submitted to the facility operator so that the numbers can be read and interpreted correctly.

Third-party application key
The third-party application key provides for migration during operation. To continue using existing third-party user media, ARIOS-2 supports the following use case:

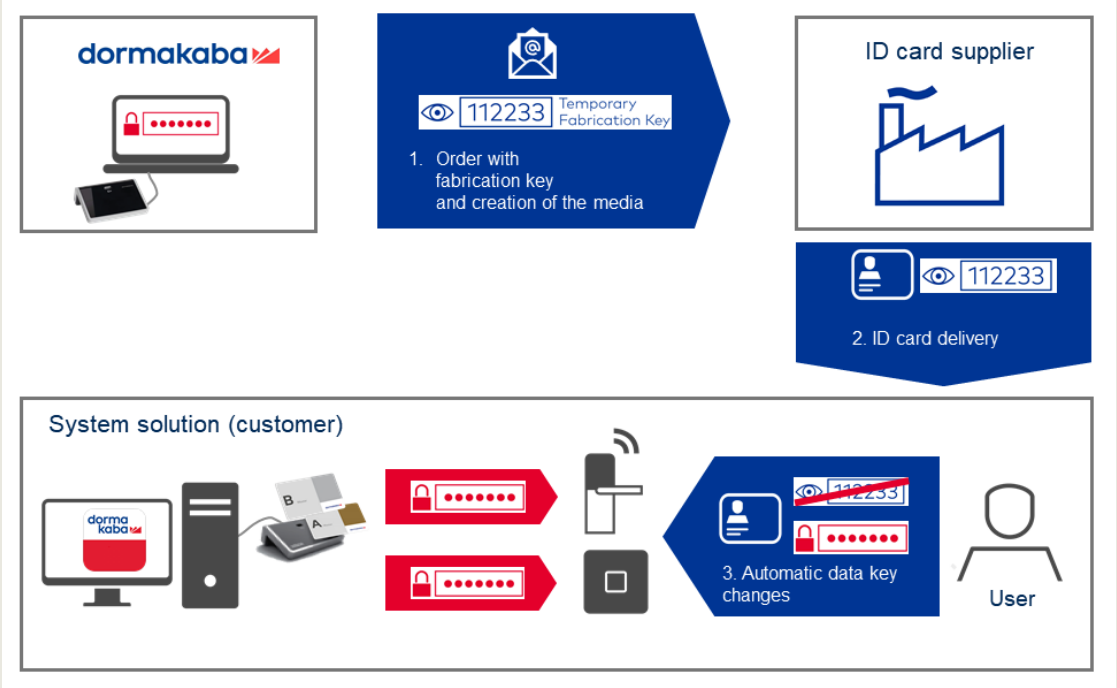
- Reading the identification number of the third-party application
  In this case, the ARIOS-2 authorization media of the system are extended by the third-party application. The third-party application key occupies memory like a site key.

The following use case is possible for the migration of existing third-party ID cards even without a third-party application key:

- Reading the identification number
  To read the ARIOS-2 identification number, the ARIOS-2 application must be applied to the user media.

Fabrication key
Creating user media represents a challenge for security in the MIFARE world. The card manufacturer is usually provided with a definition (types of ID cards) of the desired user media as well as the secret key. The card manufacturer is therefore trusted as control is not possible. The fabrication key closes this gap. Derived from the site key, the fabrication key is generated per file (Classic) or per application (DESFire) and cannot be recalculated. The fabrication key is submitted to the manufacturer with the manufacturing order. If the user medium is then used for the first time on the system application, it recognises the fabrication key and exchanges it for the unique application key per user medium and file/application on the user medium. If a media manufacturer produces the same identification twice, this would be detected and all media with this ID immediately blocked.

Secure media creation and media initialisation with the fabrication key



Any questions? We would be happy to answer any questions you may have.

dormakaba International Holding AG | Hofwisenstrasse 24 | CH-8153 Rümlang | T +41 44 818 90 11 | info@dormakaba.com | www.dormakaba.com