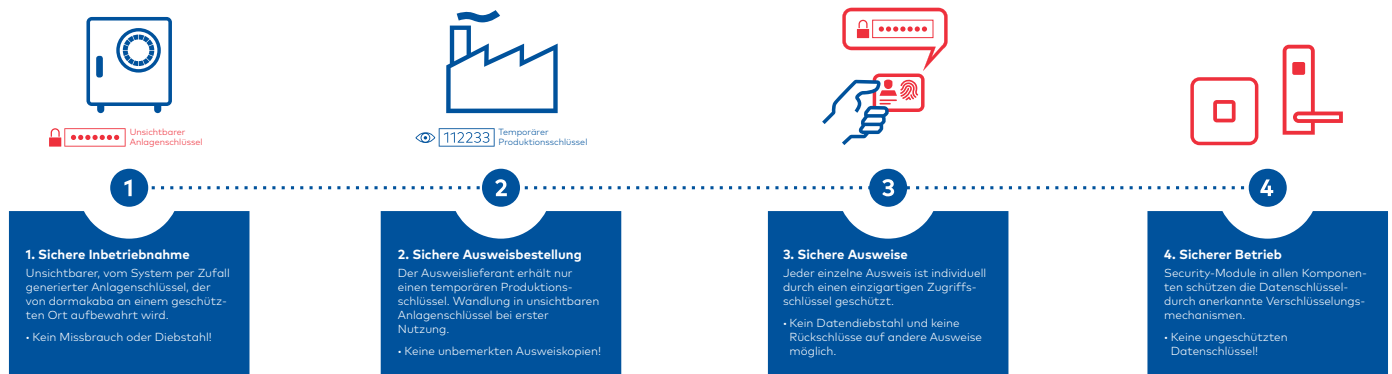




# Whitepaper MIFARE® mit ARIOS-2 Sicherheitskonzept

Warum Sie mit ARIOS-2 von dormakaba erhöhte Sicherheit für MIFARE® erhalten



# Erhöhte Sicherheit für MIFARE® mit ARIOS-2

MIFARE® ist eine dominante RFID-Technologie. Mit dem ARIOS-2 Sicherheitskonzept bietet dormakaba als Komplett-Lösungsanbieter, im Vergleich zu gängigen MIFARE®-Lösungen, zusätzliche und ausgeklügelte Mechanismen, die Ihre Zutrittskontrolle noch sicherer machen.

Ein zentrales Element von ARIOS-2 ist der eindeutige Sicherheitsschlüssel, der per Zufallsgenerator generiert wird und für niemanden ersichtlich ist. Dies gibt hohe Sicherheit in allen Prozessschritten: von der Erzeugung, Inbetriebnahme, Ausweisproduktion bis zur Wartung. So wird etwa bei den Bestellungen für Ausweise einen spezifischer Code pro Anlage für den Ausweishersteller erstellt. Erst wenn die neuen Ausweise geliefert werden, wird dieser Code in einem gesicherten ARIOS-2-Prozess in den Anlagenschlüssel gewandelt und dieser

Vorgang im System protokolliert, so dass keine illegal produzierten Ausweise unbemerkt eingesetzt werden könnten.

Zudem ist der Datenaustausch zwischen Leser und Ausweis mit den anerkannten Verfahren AES-128 (Advanced Encryption Standard) oder 3DES (Triple Data Encryption Algorithm) verschlüsselt. Dies schützt Systembetreiber vor heute gängigen Angriffsszenarien wie etwa die sogenannten Reverse Engineering Verfahren oder Man-in-The-middle-Attack.

Die ARIOS-2 Sicherheitsmechanismen reichen sogar bis in den einzelnen Ausweis. Das bedeutet, dass die Datenverschlüsselung für jeden Ausweis individuell ist. Somit hätten Angreifer ebenfalls keine Chance, Rückschlüsse auf die Verschlüsselung einer Gesamtanlage zu ziehen.

## Was ist ARIOS-2?

Das ARIOS-2 Sicherheitskonzept schließt eine Sicherheitslücke von RFID-Anwendungen, deren Sicherheitsmechanismus auf einem benutzerdefinierten Datenschlüssel beruht.

Der MIFARE®-Datenschlüssel kann ohne ARIOS-2 problemlos unbemerkt weitergegeben oder ausgespäht werden. Das ARIOS-2 Sicherheitskonzept unterstützt Anwender, ihre Datenschlüssel sicher

und einfach aufzubewahren, so dass eine unbemerkte Weitergabe oder Manipulation verhindert und der Sicherheitslevel des Systems angehoben wird.

Dieses Dokument erläutert die einzelnen Mechanismen und Kernelemente des Sicherheitskonzeptes und macht deutlich, welchen Vorteil Anwender mit ARIOS-2 für Ihre Zutrittskontrolle erhalten.

# MIFARE® mit dormakaba ARIOS-2 – Sicherheitskonzept Die Kernelemente

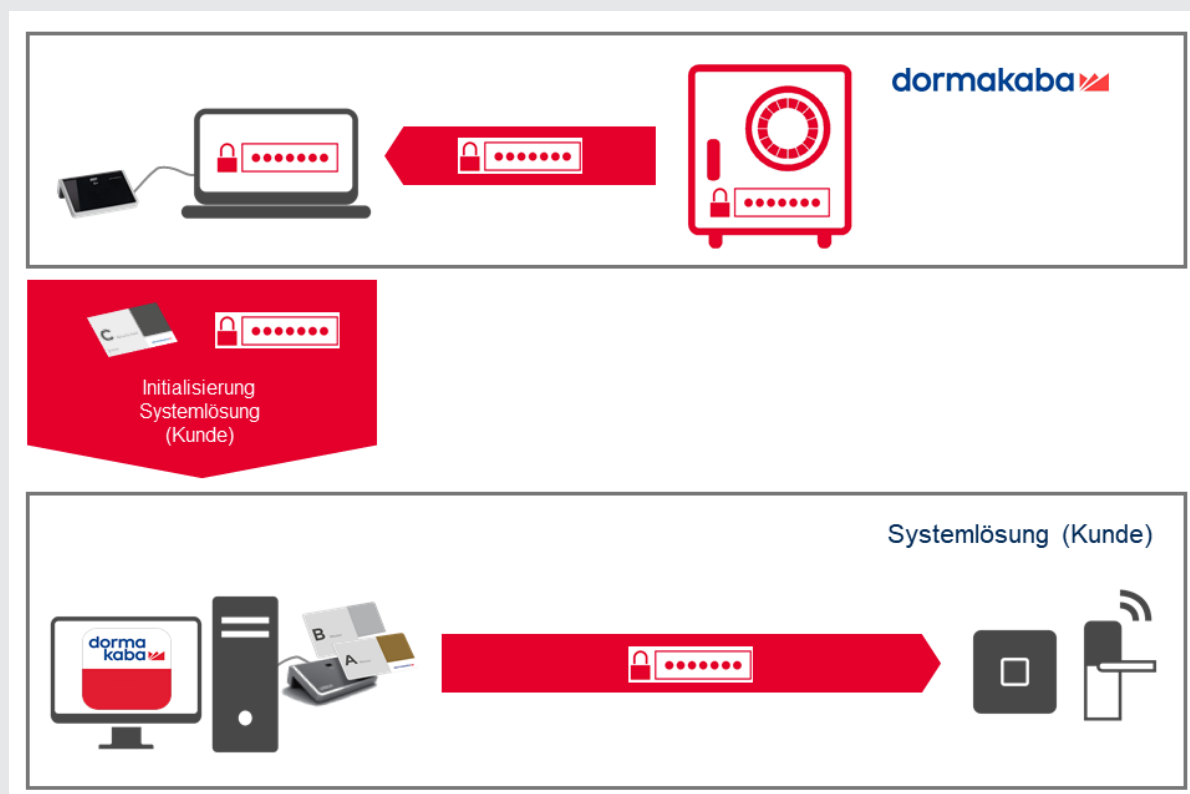
## 1. Anlageschlüssel

Das zentrale Element des MIFARE® mit ARIOS-2 Sicherheitskonzeptes ist der Anlageschlüssel. Das MIFARE® mit ARIOS-2 Konzept stellt sicher, dass der Anlageschlüssel zu keiner Zeit bekannt ist. Der kundenspezifische, geheime und nicht sichtbare Anlageschlüssel wird in einer von dormakaba speziell geschützten Umgebung von dormakaba erzeugt und sicher aufbewahrt.

Dank MIFARE® mit ARIOS-2 können mit dem Anlageschlüssel verschiedene Anlagen völlig unabhängig voneinander betrieben werden.

Zusätzliche Sicherheit bietet ARIOS-2 dadurch, dass der Anlageschlüssel nicht zur direkten Autorisierung eines Benutzermediums verwendet wird, wie sonst in MIFARE®-Anwendungen üblich. Der Anlageschlüssel liefert in ARIOS-2 die Kalkulationsbasis für die Berechnung des individuellen Zugriffsschlüssels auf ein Benutzermedium.

### Der Anlageschlüssel und die Berechtigungsmedien – niemals sichtbar und auslesbar



## 2. Berechtigungsmedien (Master Medien)

Der Anlageschlüssel wird nach der Generierung auf einem Berechtigungsmedium zur Anlage gebracht. Die Berechtigungsmedien erlauben dem Besitzer, die Anlage in Betrieb zu nehmen und Veränderungen vorzunehmen. Der grosse Vorteil eines solchen Mediums ist, dass dieses jederzeit kontrolliert genutzt werden kann und eine mündliche und schriftliche Weitergabe verhindert wird. Das Konzept basiert dadurch auf „Besitz“ und nicht auf „Wissen“ (geteiltes Geheimnis).

Im Sicherheitskonzept ARIOS-2 werden zwei Typen von Berechtigungsmedien verwendet:

- Sicherheitskarte (Typ C)
- Programmiermaster (Typ A / Typ B)

### 2.1. Sicherheitskarte C

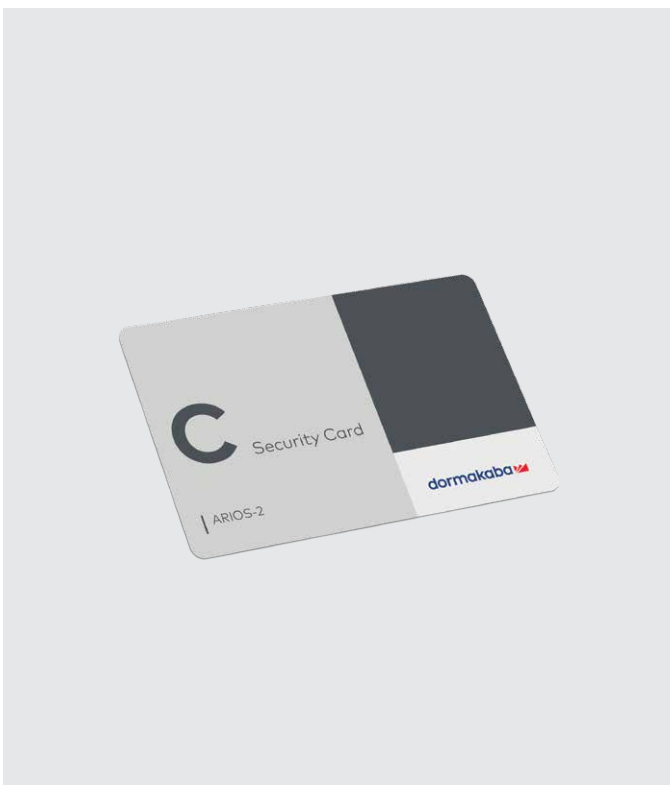
Die Sicherheitskarte C ist ein RFID-Ausweis zur Initialisierung der Systemanwendung und soll deshalb nach der Verwendung an einem sicheren Ort verwahrt werden. Die Sicherheitskarte C wird von dormakaba zur Verfügung gestellt und ist vom Typ MIFARE® DESFire®. Sicherheitsrelevante Daten wie der Anlageschlüssel und die Konfigurationsdaten sind auf der Sicherheitskarte C verschlüsselt (AES-128 oder 3DES) abgelegt. Zur Nutzung der Sicherheitskarte C ist der dormakaba Tischleser erforderlich. Bei der Inbetriebnahme wird der mit AES-128 oder 3DES

verschlüsselte Anlageschlüssel von der Sicherheitskarte bzw. Programmiermaster an alle Systemkomponenten übertragen und abgelegt. Der Anlageschlüssel ist zu keiner Zeit sichtbar. Die Übertragung erfolgt an Standalone-Komponenten mit dem Programmiermaster manuell (vor Ort), an Online-Komponenten über die Systeminfrastruktur (zentral).

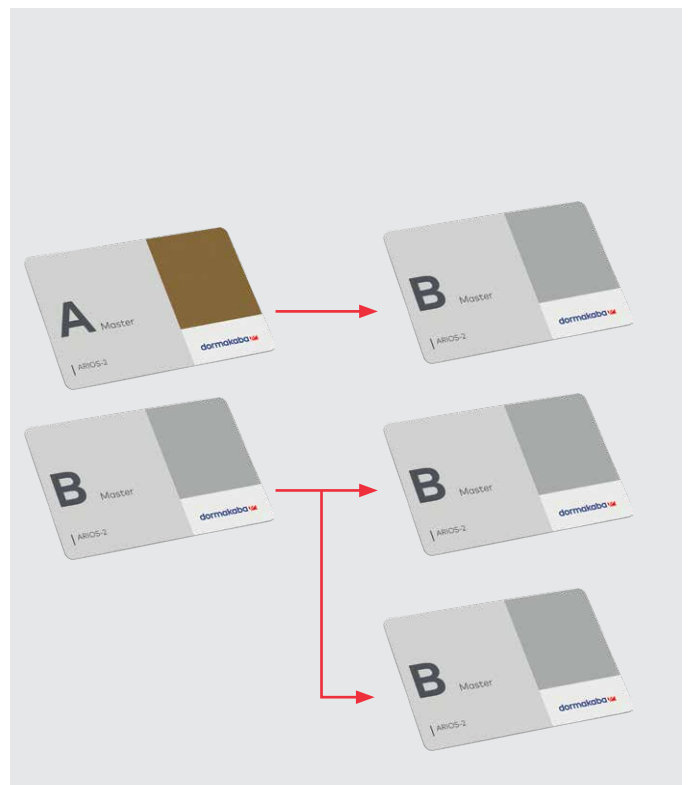
### 2.2. Programmiermaster A/B

Programmiermaster sind RFID-Ausweiskarten, mit denen standalone Komponenten initialisiert, gewartet und programmiert werden. Aus administrativen Gründen können die Inhalte an weitere Programmiermaster vererbt werden (keine Duplikate). Die Programmiermaster werden von dormakaba zur Verfügung gestellt und sind vom Typ MIFARE® DESFire®. Sicherheitsrelevante Daten wie der Anlageschlüssel sind auf dem Programmiermaster verschlüsselt (AES-128 oder 3DES) abgelegt. Zur Nutzung ist der dormakaba Tischleser erforderlich.

### Sicherheitskarte C



### Programmiermaster A und B



## Berechtigungsmedien in der Übersicht

	Sicherheitskarten	Programmiermaster
<b>Typen</b>	Typ C	Typ A / Typ B
<b>Funktionen</b>	Initialisierung von Systemanwendungen (mindestens einmal pro Anlage vorhanden)	Initialisierung von standalone-Komponenten
<b>Kann Kopien erstellen</b>	Nein	Nein (Vererbung beschränkt möglich)
<b>Medium</b>	MIFARE® DESFire® (berührungslos)	MIFARE® DESFire® (berührungslos)
<b>Dateninhalt</b>	<ul style="list-style-type: none"> <li>– Verschlüsselte Kopie von ARIOS-2 Sicherheitsdaten</li> <li>– Konfigurationsdaten der Anlage</li> </ul>	<ul style="list-style-type: none"> <li>– Verschlüsselte Kopie von ARIOS-2 Sicherheitsdaten</li> </ul>

### 3. Sicherheitschip im Tischleser

Zur Konfiguration muss die Sicherheitskarte C jeweils auf den Tischleser gelegt und ausgelesen werden. Wird die Systemanwendung oder der Arbeitsplatzrechner ausgeschaltet, gehen diese Sicherheitsdaten im Tischleser wieder verloren.

Systemanwendungen mit einer eigenen Benutzerberechtigung (z. B. exos) können die Sicherheitsdaten der Sicherheitskarte auch in der systemeigenen Datenbank ablegen. Nach dem Aufstarten des initialisierten Tischlesers werden die Sicherheitsdaten wieder geladen. Somit muss die Sicherheitskarte nur einmal bei der Inbetriebnahme dieses

Tischlesers aufgelegt werden, denn die Sicherheitsdaten sind auch in der Systemanwendung verschlüsselt. Diese Komfortfunktion erlaubt ein effizientes Arbeiten ohne Sicherheitslücken. Wird der Tischleser entwendet (von der Systemanwendung getrennt) verliert er alle Daten. Im normalen Betrieb wird dieser Tischleser zum Ausgeben und Einlesen von Medien genutzt.



# MIFARE® mit dormakaba ARIOS-2 Zugriffs- und Verschlüsselungs- mechanismen

Das automatische Generieren des Anlageschlüssel stellt sicher, dass dieser zu keinem Zeitpunkt bekannt ist. Sollte der unwahrscheinliche Fall eintreten, dass der Anlageschlüssel einer beliebigen Anlage geknackt würde, wäre dank der flachen Berechtigungsstruktur nur diese eine Anlage gefährdet und ein Rückschluss auf eine andere Anlage nicht möglich. Die Sicherheit würde wieder hergestellt, indem ein neuer Anlageschlüssel für diese Anlage generiert würde.

Für die Verteilung des Anlageschlüssels innerhalb einer Anlage sowie für den Zugriff auf Benutzermedien wird eine Verschlüsselung wie AES-128 oder 3DES verwendet. Die verwendeten Verschlüsselungsmechanismen können interessierten Systembetreibern jederzeit zugänglich gemacht werden.

## Anlageschlüssel

Der Anlageschlüssel wird mit einem einem zertifizierten Zufallsgenerator generiert.

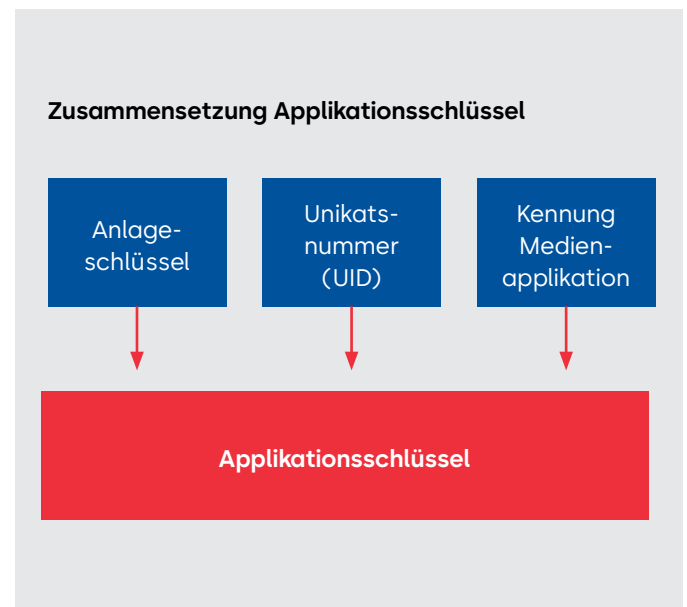
## Applikationsschlüssel

Mit dem Applikationsschlüssel erfolgt der Zugriff (Authentisierung) auf die Daten im Benutzermedium. Aus Sicherheitsgründen hat jede Applikation auf jedem Benutzermedium einen eigenen Applikationsschlüssel.

Mit dieser Methode wird eine hohe Sicherheit erreicht. Würde es gelingen, einen Applikationsschlüssel zu entschlüsseln, wäre nur diese Applikation auf diesem Benutzermedium gefährdet. Rückschlüsse auf andere Benutzermedien wären nicht möglich.

**Der Applikationsschlüssel setzt sich in der Kodierung wie folgt zusammen:**

- Anlageschlüssel der Anwendung
- Unikatsnummer des Benutzermediums
- Kennung der jeweiligen Medienapplikation



### Medien-Leseschlüssel

Dieser Schlüssel erlaubt einem Drittsystem oder einem Fremdgerät, welches das ARIOS-2 Konzept nicht unterstützt, die programmierte Identifikationsnummer auf dem Benutzermedium zu lesen. Neben diesem Medien-Leseschlüssel werden dem Betreiber noch weitere Strukturdaten übergeben, sodass die Nummer korrekt gelesen und interpretiert werden kann.

### Fremdapplikationsschlüssel

Der Fremdapplikationsschlüssel gewährleistet die Migration im laufenden Betrieb. Um bestehende Benutzermedien von Drittanbietern weiterhin zu verwenden, unterstützt ARIOS-2 folgenden Anwendungsfall:

- **Lesen der Identifikationsnummer von Fremdapplikationen**  
In diesem Fall werden die ARIOS-2 Berechtigungsmedien der Anlage mit der Fremd-Applikation erweitert. Der Fremdapplikationsschlüssel belegt einen Speicherplatz wie ein Anlageschlüssel.

Folgender Anwendungsfall ist für die Migration bestehender Fremdausweise auch ohne Fremdapplikationsschlüssel möglich:

- **Lesen der Identifikationsnummer**  
Um die ARIOS-2 Identifikationsnummer zu lesen, muss die ARIOS-2 Applikation auf die Benutzermedien aufgebracht werden.

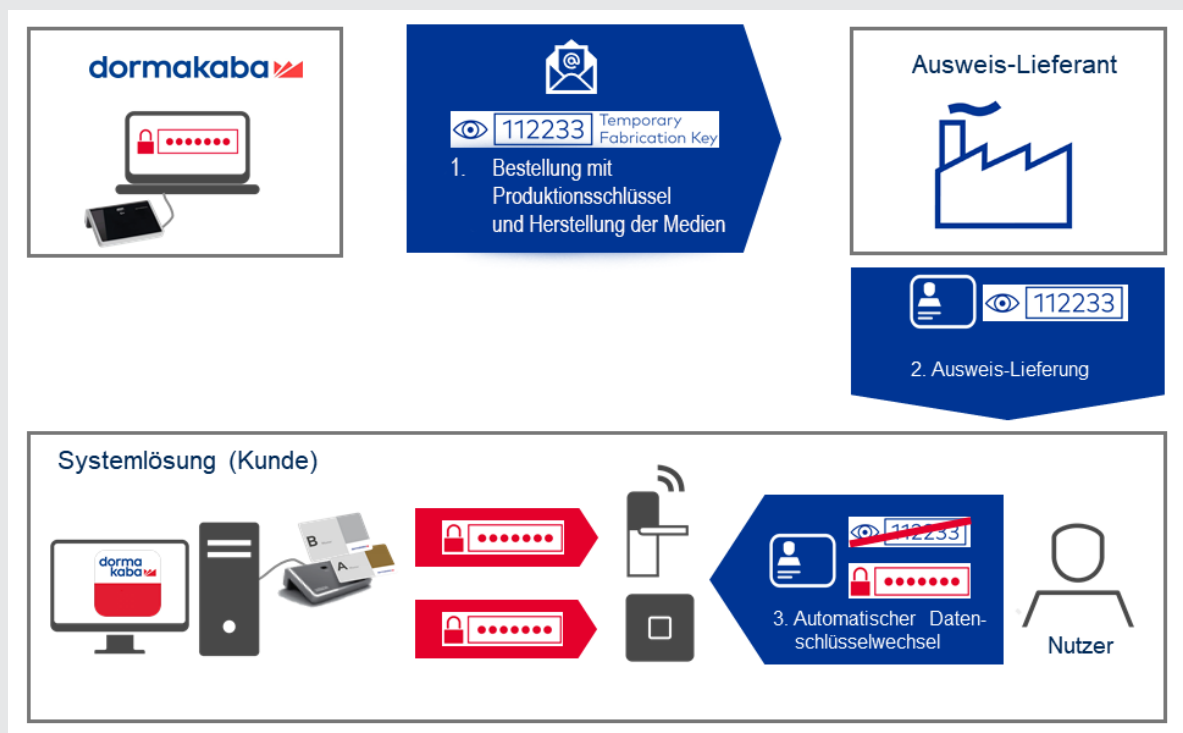
### Produktionsschlüssel

Eine Herausforderung bezüglich Sicherheit in der MIFARE®-Welt stellt die Erstellung von Benutzermedien dar. Üblicherweise werden dazu dem Kartenhersteller eine Definition (Ausweistypen) der gewünschten Benutzermedien sowie der geheime Schlüssel übergeben. Es wird also dem Kartenhersteller vertraut, eine Kontrolle ist nicht möglich. Mit dem Produktionsschlüssel wird diese Lücke geschlossen. Denn abgeleitet vom Anlageschlüssel wird der Produktionsschlüssel je File (Classic) oder Applikation (DESFire®) generiert und ist nicht rekalkulierbar.

Der Produktionsschlüssel wird dem Hersteller mit dem Herstellungsauftrag übergeben. Wird dann das Benutzermedium erstmalig an der Systemanwendung benutzt, erkennt diese den Produktionsschlüssel und tauscht diesen mit dem pro Benutzermedium und Datei/Applikation eindeutigen Applikationsschlüssel auf dem Benutzermedium aus.

Würde ein Medienhersteller die gleiche Identifikation zweimal produzieren, so würde das erkannt und alle Medien mit dieser ID sofort gesperrt.

## Sichere Medieneerstellung und Medieninitialisierung durch Produktionsschlüssel



## Unser Nachhaltigkeitsengagement

Wir setzen uns entlang unserer gesamten Wertschöpfungskette für eine nachhaltige Entwicklung ein und behalten dabei unsere ökonomische, ökologische und soziale Verantwortung gegenüber nachfolgenden Generationen stets im Blick. Nachhaltigkeit auf Produktebene ist ein wichtiger und zukunftsorientierter Ansatz im Bauwesen. Um quantifizierte Daten über Umweltauswirkungen eines Produktes entlang dessen gesamten Lebenszyklus zu geben, stellt dormakaba Umwelt-Produktdeklarationen (Environmental Product Declaration, EPD), basierend auf ganzheitlichen Ökobilanzen, bereit.

[www.dormakaba.com/sustainability](http://www.dormakaba.com/sustainability)

## Unser Angebot

### Automatische Zugangslösungen

Automatiktüren und -antriebe  
Sicherheits- und Zugangslösungen



### Elektronische Zugangslösungen

Elektronische Zutritts- und  
Zeiterfassungssysteme  
Flucht- und Rettungswegsysteme  
Hotelzutrittsysteme



### Mechanische Zugangslösungen

Türschließer  
Türtechnik  
Mechanische Schliesssysteme



### Services

Beratung und Planung  
Montage und Inbetriebnahme  
Wartung and Reparatur



WN 05523851532, DE, 11/2024

Technische Änderungen vorbehalten

© dormakaba.

MIFARE® mit ARIOS-2 von dormakaba ist abhängig von der eingesetzten dormakaba Zutrittslösung.

MIFARE® und MIFARE® DESFire® sind eine eingetragene Marken von NXP B.V.



[dormakaba.com](http://dormakaba.com)

### **dormakaba Deutschland GmbH**

DORMA Platz 1  
DE-58256 Ennepetal  
T +49 2333 793-0  
[info.de@dormakaba.com](mailto:info.de@dormakaba.com)  
**dormakaba.de**

### **dormakaba Luxembourg SA**

Duchscherstrooss 50  
LU-6868 Wecker  
T +352 26710870  
[info.lu@dormakaba.com](mailto:info.lu@dormakaba.com)  
**dormakaba.lu**

### **dormakaba Austria GmbH**

Ulrich-Bremi-Strasse 2  
AT-3130 Herzogenburg  
T +43 2782 808-0  
[office.at@dormakaba.com](mailto:office.at@dormakaba.com)  
**dormakaba.at**

### **dormakaba Schweiz AG**

Mühlebühlstrasse 23  
CH-8620 Wetzikon  
T +41 848 85 86 87  
[info.ch@dormakaba.com](mailto:info.ch@dormakaba.com)  
**dormakaba.ch**