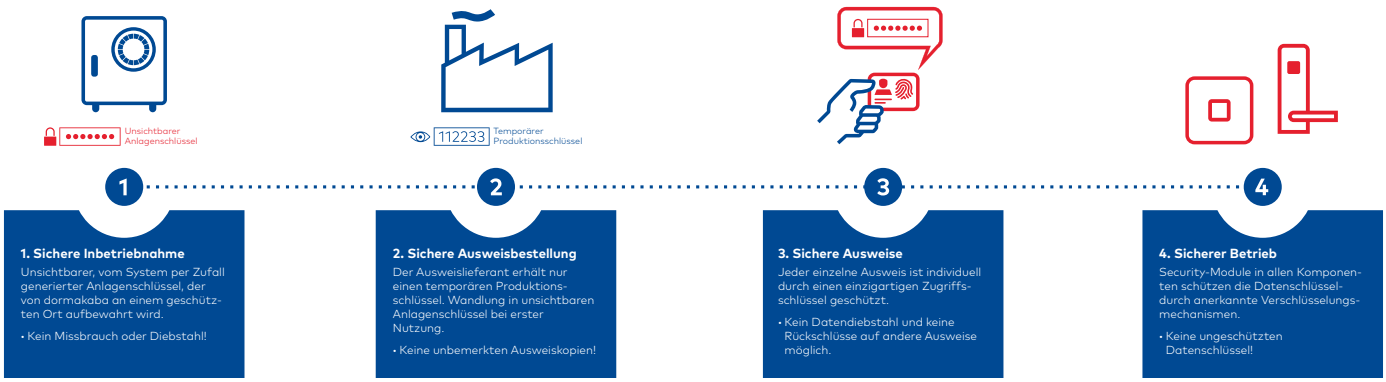
White Paper: dormakaba ARIOS-2 Sicherheitskonzept

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



MIFARE ist eine weit verbreitete RFID-Technologie. Mit dem ARIOS-2 Sicherheitskonzept bieter 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 eineindeutige 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 Ausweis-Bestellungen einen spezifischer Code pro Anlage für den Ausweis-Hersteller erstellt. Erst wenn die neuen Ausweise geliefert werden, wird dieser Code in einem gesicherten ARIOS-2-Prozess in den Anlageschlüssel 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 oder 3DES verschlüsselt. Dies schützt Systembetreiber vor heute gängigen Angriffs-szenarien 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 einem benutzerdefinierten Datenschlüssel beruht.

Der MIFARE-Datenschlüssel kann ohne ARIOS-2 problemlos unbemerkt weitergegeben oder ausspioniert 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 Sichehreitsmechnismen und Kernelemente des Sicherheitskonzeptes und macht deutlich, welchen Sicherheitsgewinn Anwender mit ARIOS-2 für Ihre Zutrittskontroll-Lösung erhalten.

dormakaba

dormakaba ARIOS-2 – Sicherheitskonzept
Die Kernelemente

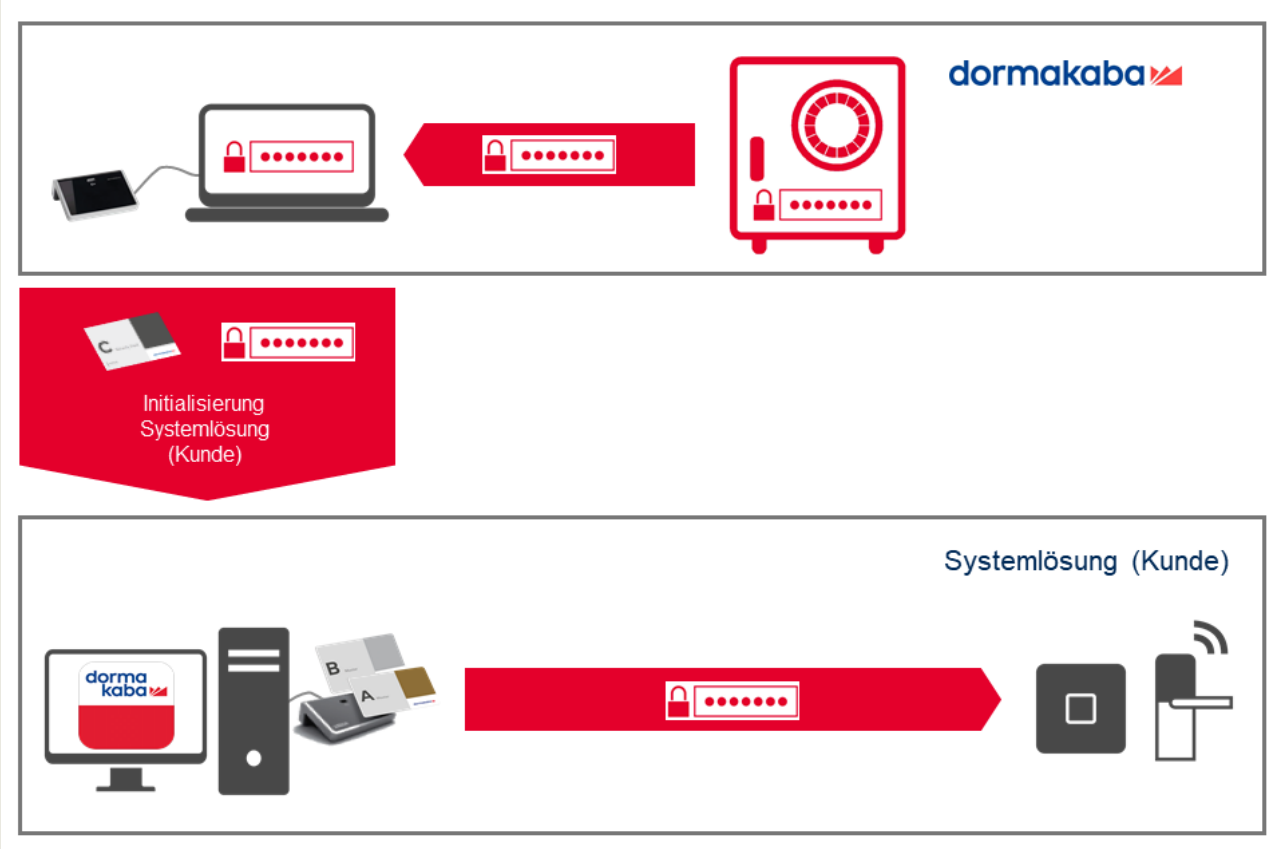
1. Anlageschlüssel

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

Mit ARIOS-2 können dank dem Anlagenschlüssel verschiedene Anlagen völlig unabhängig voneinander betrieben werden.

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

Der Anlagenschlüssel und die Berechtigungsmedien – niemals sichtbar und auslesbar



2. Berechtigungsmedien (Master Medien)

Der Anlagenschlüssel 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 Berechtigungsmediums 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

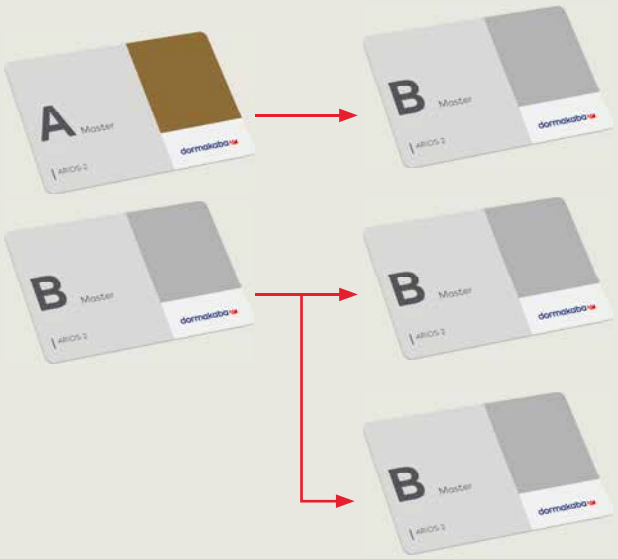
Die Sicherheitskarte C ist ein RFID-Ausweis zur Initialisierung der Systemanwendung und soll deshalb nach der Verwendung an einem sicheren Ort verwahrt werden. Die Sicherheitskarte C wird von dormakaba zur Verfügung gestellt und ist vom Typ MIFARE DESFire. Sicherheitsrelevante Daten wie der Anlageschlüssel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

Sicherheitskarte C

Programmiermaster A und B



Berechtigungsmedien in der Übersicht

	Sicherheitskarten	Programmiermaster
Typen	Typ C	Typ A / Typ B
Funktionen	Initialisierung von Systemanwendungen (mindestens einmal pro Anlage vorhanden)	Initialisierung von standalone-Komponenten
Kann Kopien erstellen	Nein	Nein (Vererbung beschränkt möglich)
Medium	MIFARE DESFire (berührungslos)	MIFARE DESFire (berührungslos)
Dateninhalt	– Verschlüsselte Kopie von ARIOS-2 Sicherheitsdaten – Konfigurationsdaten der Anlage	Verschlüsselte Kopie von ARIOS-2 Sicherheitsdaten

3. Sicherheitschip im Tischleser

Der Tischleser 91 08 MRD ist ein wichtiger Bestandteil bei der Konfiguration der Zutrittslösung. Bei der Konfiguration muss die Sicherheitskarte C jeweils auf den Tischleser gelegt und ausgelesen werden. Wird die System-anwendung oder der Arbeitsplatzrechner ausgeschaltet, gehen diese Sicherheitsdaten im Tischleser wieder verloren.

Systemanwendungen mit einer eigenen Benutzer-berechtigung (z. B. Kaba exos 9300) können die Sicher-heitsdaten 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 (3DES). 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.

dormakaba ARIOS-2
Zugriffs- und Verschlüsselungsmechanismen

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 3DES- oder AES128-Verschlüsselung verwendet. Die verwendeten Verschlüsselungsmechanismen können interessierten Systembetreibern jederzeit zugänglich gemacht werden.

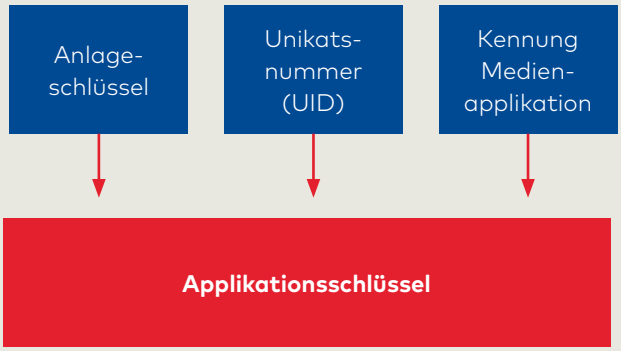
Anlageschlüssel
Der Anlageschlüssel wird mit einem einem zertifizierten Zufallsgenerator generiert.

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

Zusammensetzung Applikationsschlüssel



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:

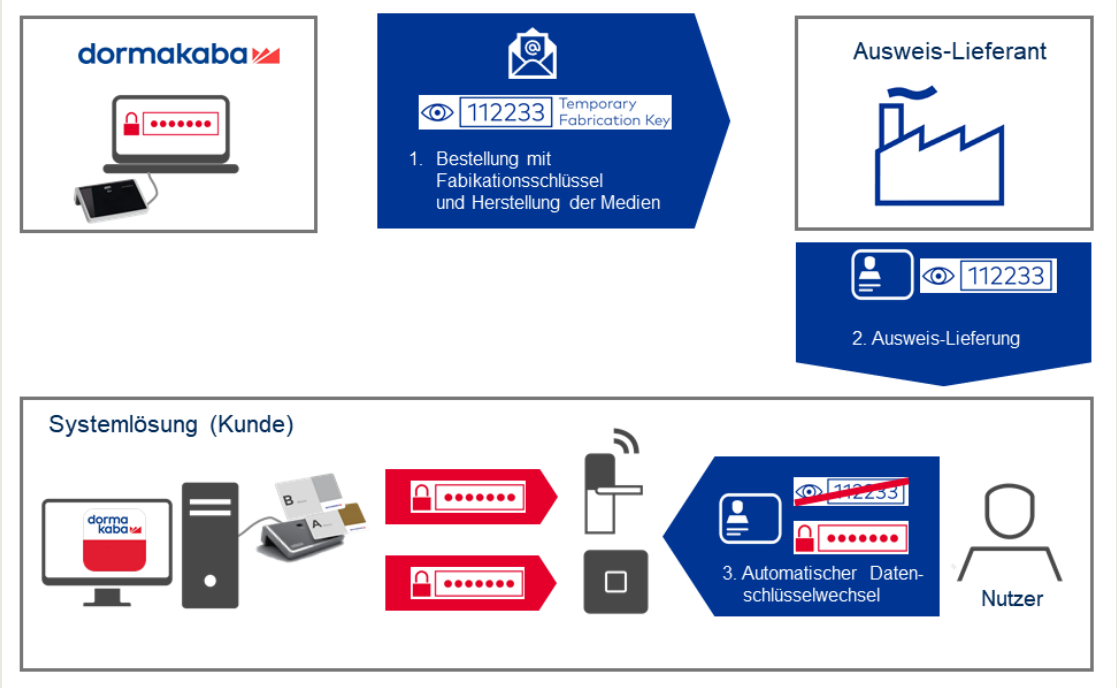
- Lesen der Identifikationsnummer von Fremd-Applikation.
  In diesem Fall werden die ARIOS-2 Berechtigungsmedien der Anlage mit der Fremd-Applikation erweitert. Der Fremdapplikationsschlüssel belegt einen Speicherplatz wie ein Anlageschlüssel.

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.

Fabrikationsschlüssel
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 Fabrikationsschlüssel wird diese Lücke geschlossen. Denn abgeleitet vom Anlageschlüssel wird der Fabrikationsschlüssel je File (Classic) oder Applikation (DESFire) generiert und ist nicht rekalkulierbar. Der Fabrikationsschlüssel wird dem Hersteller mit dem Herstellungsauftrag übergeben. Wird dann das Benutzermedium erstmalig an der Systemanwendung benutzt, erkennt diese den Fabrikationsschlüssel 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 Medienerstellung und Medieninitialisierung durch Fabrikationsschlüssel



Haben Sie Fragen? Wir beraten Sie gerne und freuen uns auf Sie.

dormakaba Deutschland GmbH | DORMA Platz 1 | DE-58256 Ennepetal | T +49 2333 793-0 | info.de@dormakaba.com | www.dormakaba.de
dormakaba Luxembourg SA | Duchscherstrooss 50 | LU-6868 Wecker | T +352 26710870 | info.lu@dormakaba.com | www.dormakaba.lu
dormakaba Austria GmbH | Ulrich-Bremi-Strasse 2 | AT-3130 Herzogenburg | T +43 2782 808-0 | office.at@dormakaba.com | www.dormakaba.at
dormakaba Schweiz AG | Mühlebühlstrasse 23 | CH-8620 Wetzikon | T +41 848 85 86 87 | info.ch@dormakaba.com | www.dormakaba.ch