dormakaba ARIOS-2

FAQ: Antworten auf die wichtigsten Fragen

1. Einleitung

Das ARIOS-2 Sicherheitskonzept schliesst eine Sicherheitslücke von RFID-Anwendungen, deren Sicherheitsmechanismus auf einem dem Systembetreiber bekannten Datenschlüssel beruht. Mit ARIOS-2 haben Angreifer keine Chance, Rückschlüsse auf die Verschlüsselung einer Gesamtanlage zu ziehen.

Dieses Dokument gibt Antworten auf die wichtigsten Fragen bezüglich der von dormakaba eingesetzten MIFARE-Technologie unter Verwendung von ARIOS-2. Das Dokument beschreibt nicht Details des ARIOS-2 Konzeptes. Dies ist in Form des ARIOS-2-Whitepaper dokumentiert, das als Grundlage für das Verständnis dieses Dokuments dient. Im Weiteren werden keine spezifischen Fragen bezüglich der MIFARE-Technologie beantwortet. Dazu wird auf die MIFARE-Publikationen verwiesen:
http://www.mifare.net/

2. Strategie

2.1 Warum bietet dormakaba MIFARE-Lösungen an?
MIFARE ist eine weit verbreitete RFID-Technologie. Mit dem ARIOS-2 Sicherheitskonzept bietet dormakaba als Komplett-Lösungsanbieter, im Vergleich zu gängigen MIFARE-Lösungen, zusätzliche und ausgeklügelte Mechanismen, welche Ihr Zutrittssystem noch sicherer machen.

3. Technologie und Kompatibilität

3.1 Worin unterscheiden sich Systeme, die mit MIFARE Standard, MIFARE mit ARIOS-2 und LEGIC betrieben werden?

Argumente	LEGIC	ARIOS-2	MIFARE Standard
Schlüsselmanagement	mehrstufig hierarchisch	einstufig	keine
Schlüssel	Physical Token	Physical Token	Wissen
Masterkarte (primär)	Standard RFID-Karte von LEGIC (inkl. hierarchischer Schlüssel); Voraussetzung: Lizenzpartner	keine	keine
Masterkarte (sekundär)	Standard (LEGIC) RFIDKarte vom Systemlieferant	Standard (MIFARE DESFire) RFID-Karte von dormakaba (ohne Schlüssel)	keine
Erzeugung Masterkarte	Lizenznehmer	dormakaba	keine
Applikationsverwaltung	je Applikation ein Definitions-file sowie eine oder mehrere Masterkarten (IAM)	alle Applikationen in einer Masterkarte	abhängig von Systemlieferant
3rd-party Applikationen (Multiapplikations-fähigkeit)	durch eigene Definition und Masterkarte ergänzbar auf gleichen Benutzermedien	unabhängig von ARIOS-2 auf gleichen Benutzer-medien (Medien offen für weitere Applikationen)	abhängig von Systemlieferant
Schlüsselgenerierung	fixer Vererbungsmechanis-mus basierend auf Geheimnis	verdeckte Generierung (random) in Hardware	freie offene/sichtbare Definition
Schlüsselspeicherung	Masterkarte und Leser-Hardware	Geschützter Bereich bei dormakaba, Masterkarte und Leser-Hardware	Papier oder lokale Datei, Leser-Hardware
Schlüsselverteilung	manuell über Masterkarte bei R/W Schutz; sonst über Leser-Chipset sichergestellt	automatisch über Systeminfrastruktur (geschützter Transport)	manuell über Konfigurations-Software
Kartenzugriff über RF-Schnittstelle	Durch Taufverfahren (Leser) kann der Zugriff auf das Medium eingeschränkt werden. Advant: offen oder DES/ 3DES, wobei Schlüssel fix vorgegeben und geheim ist Prime: proprietäres Verfahren	Classic: proprietäres Verfahren (Crypto 1) DESFire: 3DES / AES128 individuelle Schlüssel je Karte und Applikation/File	Classic: proprietäres Verfahren (Crypto 1) DESFire: 3DES / AES128 / AES256

3.2 Kann ich in den Systemlösungen Komponenten von Drittlieferanten verwenden?

Wenn die Integrationsschnittstelle dieser Fremdkomponente unsere Lösungen unterstützt und die Komponente die Programmierung eines Fremdapplikationsschlüssels zulässt, kann diese lesend genutzt werden. Wir empfehlen, solche Komponenten nicht in sicherheitsrelevanten Konfigurationen zu verwenden, z. B. Einsatz nur im Innenbereich. Um das zu ermöglichen, bietet ARIOS-2 einen „Read only key" als Teil des Konzepts an. Die Lizenzierung des ARIOS-2 Konzepts für Dritte ist nicht beabsichtigt.

3.3 Kann ich eine dormakaba MIFARE-Karte auch mit anderen Systemen nutzen?
MIFARE DESFire: Ja, sofern genügend Speicherplatz vorhanden ist und der PICC Master Key zur Verfügung gestellt wird.
MIFARE Classic: Ja, sofern die UID, MAD oder ein freier Sektor verwendet wird.

3.4 Kann ich eine MIFARE-Datenstruktur eines Drittanbieters mit dormakaba-Systemen nutzen?
Ja, wenn der „Read only key" des Kunden bekannt ist sowie eine eindeutige Ausweisnummer existiert.

3.5 Kann ich ein installiertes dormakaba System durch ARIOS-2 erweitern?
Eine Erweiterung ist möglich. Die bestehenden Komponenten werden aber nicht über das ARIOS-2 Sicherheitskonzept verfügen. Bei einem Parallelbetrieb muss zu der bestehenden Datenstruktur die ARIOS-2 Applikation auf das Benutzermedium aufgebracht werden.

Wird das dormakaba Sicherheitskonzept benötigt, so sind folgende Änderungen nötig:
- Bestehende Hardware muss ausgetauscht werden, falls diese das ARIOS-2 Sicherheitskonzept nicht unterstützen.
- Die Software ist zu aktualisieren.
- Medien müssen mit einer zusätzlichen Datenstruktur versehen werden. Dies erfolgt normalerweise mit einer Kiosklösung. Dazu muss genügend freier Medienspeicher verfügbar sein.

Bei Anlagen von Drittanbietern muss die notwendige Anpassung projektspezifisch abgeklärt werden!

3.6 Kann ich Fremdapplikationen z. B. für Kantinen oder Fremdsysteme mit ARIOS-2 verwenden.
Nein, die Codierung ist auf die ARIOS-2 Applikationen beschränkt. Dazu ist ein Drittsystem zu verwenden.

3.7 Welche Medien werden von den unterschiedlichen Lösungen grundsätzlich unterstützt?
Nähere Informationen erhalten Sie in der folgenden Tabelle.

Tabelle zu 3.7 Welche Medien werden von den unterschiedlichen Lösungen grundsätzlich unterstützt?

	LEGIC	ARIOS-2	MIFARE Standard
Unterstützte RFID-Technologien	LEGIC advant: ISO 14443 A ISO 15693 LEGIC prime: LEGIC RF	MIFARE Classic 1k, 4k MIFARE DESFire 8k (standard), 4k, 2k ISO 14443 A (nur UID) weitere möglich	MIFARE Classic MIFARE DESFire
Medienbezug	von LEGIC Lizenznehmer	beliebige Kartenhersteller	beliebige Kartenhersteller
Medien-programmierung	freie Konfiguration innerhalb der LEGIC Rules (Lizenzgeber empfiehlt); einige Standards für herstellerunabhängige Kompatibilität	Wahl aus fixen proprietären Definitionen (Sicherstellung der Kompatibilität zwischen ARIOS-2 kompatiblen Systemen, abgestimmt mit Medienlieferanten. Dadurch einfache Handhabung, nur minimales Know-how notwendig)	freie Konfiguration innerhalb der MIFARE Rules, gemäss Definition Systemanbieter; keine Standards
Mittel zur Medien-programmierung	SW: LEGIC CSW oder eigene Tools der Lizenznehmer + spezielle HW	Programmiertool (Empfehlung: UniC10)	systemlieferantabhängig
Autorisierung zur Medien-programmierung	anlagenindividuelle Masterkarte bei Kartenprogrammier-Station physikalisch notwendig	File mit individuellem Fabrikationsschlüssel (Wissen); nicht identisch mit Anlageschlüssel.	Anlagenschlüssel (Wissen) oder systemlieferantabhängige Lösung
Organisatorische Sicherheit:	basierend auf "Besitz" **advant**: Technisch sicher (keine publizierten Sicherheitslücken) **prime**: Technisch beschränkt sicher (bekannte publizierte Sicherheitslücken)	basierend auf "Besitz" **DESFire**: Technisch sicher (keine publizierten Sicherheitslücken) **Classic**: Technisch beschränkt sicher (bekannte publizierte Sicherheitslücken)	basierend auf "Wissen" (i.d.R. sicherheitskritischer) **DESFire**: Technisch sicher (keine publizierten Sicherheitslücken) **Classic**: Beschränkt sicher (bekannte publizierte Sicherheitslücken)

3.8 Können Classic und DESFire Karten in einem System parallel benutzt werden?

Ja.
Aus Sicherheitsgründen wird der Einsatz von DESFire Medien empfohlen. Zudem ist die Unterstützung von Medien-Tracebacks nur mit DESFire Medien gegeben.
Allgemeine Voraussetzungen:

- genügend Speicher auf dem bestehenden Medium verfügbar
- Zugriffscode (schreiben/lesen) für Karte vorhanden.

Als Kiosklösung wird ein Gerät bezeichnet, welches die ARIOS-2 Applikation auf bestehende Karten aufbringt. Dieses Gerät ist beim Kunden installiert.

Tabelle zu 3.8: Parallele Nutzung von unterschiedlichen MIFARE-Technologien

Ausgangslage	Wechsel zu MIFARE Classic ARIOS-2	Wechsel zu MIFARE DESFire ARIOS-2
MIFARE Classic	**Bestehende Karte** 1. Zusatzcodierung 2. Kiosklösung notwendig 3. Leser-Hardware tauschen **Kartentausch im laufenden Betrieb** 1. Leser-Hardware tauschen 2. neue Karten ausrollen	**Kartentausch im laufenden Betrieb** 1. Leser-Hardware tauschen 2. neue Benutzerkarten ausrollen
MIFARE Classic ARIOS-2		**Kartentausch im laufenden Betrieb** Mischbetrieb abhängig von System und Konfiguration 1. Neue Masterkarte 2. Neue Benutzerkarten ausrollen
MIFARE DESFire		**Bestehende Karte** Mischbetrieb abhängig von System und Konfiguration. 1. Zusatzcodierung 2. Kiosklösung notwendig 3. Leser-Hardware tauschen **Kartentausch im laufenden Betrieb** Mischbetrieb abhängig von System und Konfiguration. 1. Leser-Hardware tauschen 2. neue Benutzerkarten ausrollen

4. Sicherheit

4.1 Kann eine MIFARE Classic Karte 1:1 kopiert oder verändert werden?
Bekanntlich wurde der Sicherheitscode der MIFARE Classic Karte entschlüsselt. Dies bedeutet jedoch nicht, dass MIFARE Classic Karten mit ARIOS-2 unsicher sind. Um eine Manipulation durchzuführen, müssen einerseits die Kenntnisse, Methoden und Tools für den MIFARE Hack bekannt sein und andererseits ein Zugang zu einem Leser in einer Anlage bestehen, mit dem Ziel, Daten über den Verbindungsaufbau zu sammeln und den Applikations- schlüssel zu bestimmen

Die ARIOS-2 Komponenten verfügen jedoch über Mechanismen, welche dies erschweren durch:
- Verzögerung der Authentisierung,
- Verzögerung durch Aufweckschaltung bei standalone Komponenten,
- Verwendung verschiedener Schlüssel.

4.2 Wie funktioniert das Sicherheitskonzept?
Im Wesentlichen basiert das Sicherheitskonzept auf einem sicheren Schlüsselspeicher, in dem alle Schlüssel wie in einem Tresor gespeichert sind. Von aussen ist es nicht möglich, auf diese Schlüssel direkt zuzugreifen. Dieser Schlüsselspeicher ist in einer Sicherheitskarte (Anlagenschlüssel) und in jeder Anlagenkomponente wie Leser, standalone Komponente usw. enthalten. Das ARIOS-2 Sicherheitskonzept ist im Detail aus ARIOS-2-Whitepaper zu entnehmen.

4.3 Wie unterscheidet sich das ARIOS-2 Sicherheitskonzept von den Mitbewerbern?
ARIOS-2 ist ein Sicherheitskonzept von dormakaba, welches einerseits unabhängig von der gewählten RFID-Technologie besteht und andererseits zusätzliche Schutzmechanismen zu der eingesetzten RFID-Technologie bietet.

Dies sind:
1. Sichere Inbetriebnahme
   Unsichtbarer, vom System per Zufall generierter Anlagenschlüssel, der von dormakaba an einem geschützten Ort aufbewahrt wird.
   --> Kein Missbrauch oder Diebstahl!
2. Sichere Ausweisbestellung
   Der Ausweislieferant erhält nur einen temporären Produktionsschlüssel. Wandlung in unsichtbaren Anlagenschlüssel bei erster Nutzung.
   --> Keine unbemerkten Ausweiskopien!
3. Sichere Ausweise
   Jeder einzelne Ausweis ist individuell durch einen einzigartigen Zugriffsschlüssel geschützt.
   --> Kein Datendiebstahl und keine Rückschlüsse auf andere Ausweise möglich!
4. Sicherer Betrieb
   Security-Module in allen Komponenten schützen die Datenschlüssel durch anerkannte Verschlüsselungs-mechanismen.
   --> Keine ungeschützten Datenschlüssel!

Tabelle zu 4.1: Anlagensicherheit im Vergleich

	MIFARE Classic Standard	MIFARE Classic ARIOS-2
Alle Karten haben den gleichen Applikationsschlüssel.	Dies entspricht dem häufigsten Anwendungsfall. Medien können ohne grosse Hindernisse kopiert werden.	nicht verwendet
Jede Karte hat einen eigenen Applikationsschlüssel.	Es gibt MIFARE Geräteanbieter, die über einen zusätzlichen Schutz verfügen, ähnlich ARIOS-2. Damit kann nur eine Karte kopiert werden. Die Sicherheit ist von der Applikation abhängig.	Mit ARIOS-2 verfügt jedes Medium über einen eigenen Schlüssel (Application Key). Die Sicherheit wird zusätzlich erhöht, indem der Application Key von der UID der Benutzerkarte abhängt.

4.4 Welche Medienapplikationen basieren auf dem ARIOS-2 Sicherheitskonzept?
Die Zutrittsdaten sind ähnlich wie bei LEGIC in einer Datenstruktur gespeichert. In der Tabelle unten ist der Vergleich zu den bekannten LEGIC-Segmenten dargestellt.

4.5 Wie schützt sich ARIOS-2 gegenüber den verschiedenen Angriffsarten?
Die Mechanismen sind in Kap. 4.2 und 4.3 beschrieben. Weitere Angaben sind dem Dokument ARIOS-2 Whitepaper zu entnehmen.

4.6 Wie sicher ist ein UID Betrieb?
Der ISO 14443A Standard bietet im UID Betrieb keine Sicherheit. Im Falle ARIOS-2 wird eine Methode „Save UID" unterstützt. Mit dieser Methode wird zusätzlich zur UID ein Datenpaket (KCA) [2] aus dem Medium ausgelesen. Durch ein verschlüsseltes Verfahren wird nun die Zutrittsberechtigung ermittelt. Wird nun eine UIDohne KCA simuliert, kann der Zutrittscode nicht ermittelt werden.

4.7 Muss dem Kartenhersteller ein Schlüssel abgegeben werden?
An den Kartenhersteller wird ein Fabrikationsschlüssel abgegeben. Dieser Schlüssel wird nur für die Produktion von Karten verwendet. Wird eine Karte in die Anlage integriert, so wird der Fabrikationsschlüssel durch den Applikationsschlüssel ersetzt. Dieser Vorgang wird durch das System geprüft und protokolliert. Dadurch wird ein allfälliges durch den Kartenhersteller erzeugtes Duplikat erkannt, da diese Wandlung des Schlüssels für eine Benutzerkarte mit derselben UID nur einmal gemacht werden kann.

Tabelle zu 4.4: Datenstruktur dormakaba ARIOS-2

Konfiguration

LEGIC Segemente	**MIFARE Classic ARIOS-2 Datei**	**MIFARE DESFire ARIOS-2 Applikationen**
Kaba Group Header	Identifikations-Datei	Access Applikation
CardLink	CardLink Data CardLink Aktuator Status	CardLink Data CardLink Aktuator Status Traceback
LockerLock Free selection	LockerLock Free selection	LockerLock Free selection
Biometrie		Biometrie Applikation

Nicht enthalten ist z. B. das Cash-Segment, da diese Anwendungen von Drittanbietern geliefert werden.

5. MIFARE Medien

5.1 Welche Benutzermedien können eingesetzt werden?
In der Anlage wird empfohlen, jeweils Benutzermedien des gleichen Typs einzusetzen. Die Hersteller können variieren. Die Lesedistanz kann je nach Hersteller variieren, da die Produktionsverfahren nicht standardisiert sind. Im Fall MIFARE empfehlen wir, nur Karten von Herstellern zu verwenden, die „MIFARE zertifiziert" sind.

5.2 Wer kann Karten codieren?
Jeder Kartenhersteller kann mit dem Fabrikationsschlüssel Karten codieren.

5.3 Wo kann die Karte beschafft werden?
Grundsätzlich können die Benutzermedien bei jedem Kartenlieferanten oder bei dormakaba beschafft werden. dormakaba liefert ausschliesslich Medien mit der empfohlenen MIFARE DESFire-Technologie.
Die Sicherheitskarten und Programmiermaster werden ausschliesslich von dormakaba geliefert.

5.4 Kann ich nach der Erstlieferung den Kartenlieferanten wechseln?
Ja.

Bei einem Wechsel müssen dem Kartenhersteller die folgenden Informationen zur Verfügung gestellt werden:
- AEF File (XML Format) oder Print-Information (PDF Format), erstellt mit Media-Workstation (MWS)

5.5 Kann eine bestehende MIFARE Classic oder DESFire Karte eingesetzt werden?
Ja, als Grundvoraussetzung muss zwingend der Medien-Wartungsschlüssel bekannt sein.

Wir unterscheiden zwei Fälle:
1. Die ARIOS-2 Applikation soll (Terminal) auf das bestehende Medium aufgebracht werden. Dafür muss genügend freier Speicherplatz auf dem Medium vorhanden sein.
2. Es soll die bestehende programmierte Nummer gelesen werden können. Dazu muss die Codierung der Nummer bekannt sein.

Details dazu sind mit den ARIOS-2 Spezialisten zu klären.

Tabelle zu 5.1: Welche Benutzermedien können mit ARIOS-2 eingesetzt werden?

Kartentyp	Speichergrösse[2]	Unterstützte System-Applikationen
MIFARE DESFire EV1/EV2	8kB empfohlen 2kB und 4kB möglich	CardLink (KXA) UID-geschützt (KCA)
MIFARE Classic	1kB, 4kB	CardLink UID-geschützt (KCA)

[2] In einer Anlage können Karten mit unterschiedlichen Speichergrössen eingesetzt werden.