dormakaba ARIOS-2

FAQ: risposte alle domande più importanti

1. Introduzione

Il concetto di sicurezza ARIOS-2 risolve una vulnerabilità delle applicazioni RFID il cui meccanismo di sicurezza si basa su una chiave dati nota al gestore del sistema. Con ARIOS-2, i malintenzionati non hanno alcuna possibilità di risalire alle informazioni sulla crittografia di un intero impianto.

Questo documento fornisce risposte alle domande più importanti riguardanti la tecnologia MIFARE utilizzata da dormakaba nell'ambito di ARIOS-2.
Il presente documento non descrive nel dettaglio il concetto di ARIOS-2; esso è infatti illustrato nel White paper ARIOS-2, che serve come base per la comprensione di questo documento. Nelle pagine seguenti, non verranno date risposte a domande specifiche sulla tecnologia MIFARE. A tal scopo, si rimanda alle pubblicazioni MIFARE:
http://www.mifare.net/

2. Strategia

2.1 Perché dormakaba offre soluzioni MIFARE?
MIFARE è una tecnologia RFID ampiamente diffusa. Con il concetto di sicurezza ARIOS-2, dormakaba, in qualità di fornitore di soluzioni complete, offre ulteriori meccanismi sofisticati rispetto alle comuni soluzioni MIFARE, rendendo il vostro sistema di accesso ancora più sicuro.

3. Tecnologia e compatibilità

3.1 In cosa differiscono i sistemi gestiti con MIFARE Standard, MIFARE con ARIOS-2 e LEGIC?

Argomenti	LEGIC	ARIOS-2	MIFARE Standard
Gestione delle chiavi	più livelli gerarchici	livello unico	Nessuno
Chiave	Token fisico	Token fisico	Conoscenza
Scheda master (primaria)	Scheda RFID standard di LEGIC (inclusa chiave gerarchica); requisito: partner di licenza	Nessuna	Nessuna
Scheda master (secondaria)	Scheda RFID standard (LEGIC) del fornitore del sistema	Standard (MIFARE DESFire) Scheda RFID di dormakaba (senza chiave)	Nessuna
Generazione della scheda master	Licenziatario	dormakaba	Nessuna
Gestione delle applicazioni	un file di definizione per ogni applicazione e una o più schede master (IAM)	tutte le applicazioni in una scheda master	a seconda del fornitore del sistema
Applicazioni di terze parti (capacità multiapplicativa)	può essere integrato con una definizione propria e una scheda master sugli stessi supporti utente	indipendente da ARIOS-2 sugli stessi supporti utente (supporti aperti per ulteriori applicazioni)	a seconda del fornitore del sistema
Generazione delle chiavi	meccanismo fisso di ereditarietà basato sulla segretezza	generazione nascosta (random) nell'hardware	definizione libera aperta/visibile
Memorizzazione delle chiavi	Hardware della scheda master e del lettore	Area protetta presso dormakaba, Hardware della scheda master e del lettore	Carta o file locale, Hardware del lettore
Assegnazione delle chiavi	manuale tramite scheda master con protezione R/W; altrimenti garantita tramite chipset del lettore	automatica attraverso l'infrastruttura del sistema (trasferimento protetto)	manuale tramite software di configurazione
Accesso alla scheda tramite interfaccia RF	L'accesso al supporto può essere limitato attraverso l'inizializzazione (lettore). Advant: aperto o DES/3DES, laddove la chiave è fissa di default e segreta Prime: processo proprietario	Classic: processo proprietario (Crypto 1) DESFire: 3DES/AES128 chiavi individuali per scheda e applicazione/file	Classic: processo proprietario (Crypto 1) DESFire: 3DES/AES128/AES256

3.2 È possibile utilizzare componenti di fornitori terzi nelle soluzioni di sistema?
Se l'interfaccia di integrazione del componente di terze parti supporta le nostre soluzioni e il componente consente la programmazione di una chiave delle applicazioni di terze parti, allora le componenti di fornitori terzi possono essere utilizzate in sola lettura. Si consiglia di non utilizzare tali componenti in configurazioni rilevanti per la sicurezza, ad es. uso solo in ambienti interni. A tal fine, ARIOS-2 offre una "Read only key" come parte del concetto. La concessione in licenza del concetto ARIOS-2 per terzi non è prevista.

3.3 È possibile utilizzare una scheda MIFARE dormakaba anche con altri sistemi?
MIFARE DESFire: sì, a condizione che vi sia memoria sufficiente e che venga fornita la master key PICC.
MIFARE Classic: sì, a condizione che si utilizzi l'UID, il MAD o un settore libero.

3.4 È possibile utilizzare una struttura dati MIFARE di un fornitore terzo con i sistemi dormakaba?
sì, se la "Read only key" del cliente è nota ed esiste un numero scheda ID univoco.

3.5 È possibile ampliare con ARIOS-2 un sistema dormakaba già installato?
Un ampliamento è possibile. Tuttavia, i componenti esistenti non disporranno del concetto di sicurezza ARIOS-2. Per il funzionamento in parallelo, l'applicazione ARIOS-2 deve essere aggiunta alla struttura dati esistente sul supporto utente.

Se si rende necessario il concetto di sicurezza dormakaba, si devono apportare le seguenti modifiche:
- l'hardware esistente deve essere sostituito se non supporta il concetto di sicurezza ARIOS-2.
- Il software deve essere aggiornato.
- I supporti devono essere dotati di una struttura dati supplementare. Questo avviene normalmente tramite una soluzione per chioschi informatici. A tal scopo, deve essere disponibile sufficiente memoria libera del supporto.

Nel caso di impianti di fornitori terzi, è necessario chiarire preventivamente gli adeguamenti necessari in base al progetto specifico!

3.6 È possibile utilizzare applicazioni di terze parti per mense o sistemi di terze parte con ARIOS-2?
No, la codifica è limitata alle applicazioni ARIOS-2. A tale scopo, deve essere utilizzato un sistema di terze parti.

3.7 Quali supporti sono fondamentalmente compatibili con le diverse soluzioni?
La tabella seguente fornisce ulteriori informazioni.

Tabella di 3.7 Quali supporti sono fondamentalmente compatibili con le diverse soluzioni?

	LEGIC	ARIOS-2	MIFARE Standard
Tecnologie RFID supportate	LEGIC advant ISO 14443 A ISO 15693 LEGIC prime: LEGIC RF	MIFARE Classic 1k, 4k MIFARE DESFire 8k (standard), 4k, 2k ISO 14443 A (solo UID) e possibilmente altre	MIFARE Classic MIFARE DESFire
Riferimento ai supporti	da Licenziatario LEGIC	qualsiasi produttore di schede	qualsiasi produttore di schede
Programmazione dei supporti	configurazione libera nell'ambito delle regole LEGIC (raccomandazioni del licenziante); alcuni standard per la compatibilità indipendente dal produttore	Scelta di definizioni proprietarie fisse (garanzia di compatibilità tra sistemi compatibili con ARIOS-2, concordata con i fornitori di supporti. Questo garantisce maggior facilità d'uso, si richiede solo un minimo di know-how)	Configurazione libera nell'ambito delle MIFARE Rules, in base alla definizione del fornitore del sistema; nessuno standard
Strumenti di programmazione dei supporti	SW: LEGIC CSW o strumenti propri del licenziatario + HW speciale	Strumento di programmazione (raccomandazione: UniC10)	a seconda del fornitore del sistema
Autorizzazione per la programmazione dei supporti	scheda master specifica dell'impianto fisicamente necessaria per la stazione di programmazione della scheda	File con chiave di fabbrica individuale (conoscenza); diversa dalla chiave impianto.	Chiave impianto (conoscenza) o soluzione dipendente dal fornitore del sistema
Sicurezza organizzativa:	basata sul "possesso" **advant**: tecnicamente sicuro (nessuna vulnerabilità pubblicata in termini di sicurezza) **prime**: limiti tecnici in termini di sicurezza (vulnerabilità note pubblicate)	basata sul "possesso" **DESFire**: tecnicamente sicuro (nessuna vulnerabilità pubblicata in termini di sicurezza) **Classic**: limiti tecnici in termini di sicurezza (vulnerabilità note pubblicate)	basata sulla "conoscenza" (in genere, critico dal punto di vista della sicurezza) **DESFire**: tecnicamente sicuro (nessuna vulnerabilità pubblicata in termini di sicurezza) **Classic**: sicurezza limitata (vulnerabilità note pubblicate)

3.8 Le schede Classic e DESFire possono essere utilizzate parallelamente in un sistema?

Sì.

Per motivi di sicurezza, si raccomanda l'uso di supporti DESFire. Inoltre, i traceback sono compatibili solo con i supporti DESFire.

Requisiti generali:

- sufficiente memoria disponibile sul supporto esistente
- codice di accesso (scrittura/lettura) per la scheda disponibile.

Una soluzione per chioschi informatici consiste in un dispositivo che aggiunge l'applicazione ARIOS-2 alle schede esistenti.

Tale dispositivo è installato presso il cliente.

Tabella di 3.8: uso parallelo di diverse tecnologie MIFARE

Situazione iniziale	Passaggio a MIFARE Classic ARIOS-2	Passaggio a MIFARE DESFire ARIOS-2
MIFARE Classic	**Scheda esistente** 1. Codifica supplementare 2. Soluzione per chioschi informatici necessaria 3. Sostituzione hardware del lettore **Sostituzione delle schede durante il funzionamento** 1. Sostituzione hardware del lettore 2. Eseguire il roll-out delle nuove schede	**Sostituzione delle schede durante il funzionamento** 1. Sostituzione hardware del lettore 2. Eseguire il roll-out delle nuove schede utente
MIFARE Classic ARIOS-2		**Sostituzione delle schede durante il funzionamento** Funzionamento misto a seconda del sistema e della configurazione 1. Nuova scheda master 2. Eseguire il roll-out delle nuove schede utente
MIFARE DESFire		**Scheda esistente** Funzionamento misto a seconda del sistema e della configurazione. 1. Codifica supplementare 2. Soluzione per chioschi informatici necessaria 3. Sostituzione hardware del lettore **Sostituzione delle schede durante il funzionamento** Funzionamento misto a seconda del sistema e della configurazione. 1. Sostituzione hardware del lettore 2. Eseguire il roll-out delle nuove schede utente

4. Sicurezza

4.1 È possibile copiare o modificare una scheda MIFARE Classic 1:1?

Come è noto, il codice di sicurezza della scheda MIFARE Classic è stato decodificato. Tuttavia, questo non significa che le schede MIFARE Classic con ARIOS-2 non siano sicure. Per effettuare una manipolazione, si devono innanzitutto avere le abilità nonché conoscere i metodi e gli strumenti per hackerare MIFARE; inoltre è necessario avere accesso a un lettore di un impianto con l'obiettivo di raccogliere dati sull'instaurazione del collegamento e determinare la chiave delle applicazioni.

Tuttavia, i componenti di ARIOS-2 dispongono di meccanismi che rendono tutto ciò più difficile, grazie a:

- un delay di autenticazione,
- un delay dovuto al circuito di wake-up per i componenti stand-alone,
- l'uso di diverse chiavi.

4.2 Come funziona il concetto di sicurezza?

In sostanza, il concetto di sicurezza si basa su una memoria delle chiavi sicura, in cui tutte le chiavi sono conservate come in una cassaforte. Dall'esterno non è possibile accedere direttamente alle chiavi. Tale memoria delle chiavi è contenuta in una tessera di sicurezza (chiave impianto) e in ogni componente dell'impianto come lettore, componente stand-alone ecc. Il concetto di sicurezza ARIOS-2 è illustrato in dettaglio nel White paper ARIOS-2.

4.3 Come si distingue il concetto di sicurezza ARIOS-2 dalla concorrenza?

ARIOS-2 è un concetto di sicurezza di dormakaba in grado di esistere indipendentemente dalla tecnologia RFID scelta. Inoltre, offre meccanismi di protezione supplementari alla tecnologia RFID utilizzata.

Tali meccanismi includono:

1. funzionamento sicuro:
   chiave impianto invisibile, generata casualmente dal sistema e custodita da dormakaba in un luogo protetto.
   --> Stop a uso improprio o furto!
2. Ordine sicuro della scheda ID:
   il fornitore della scheda ID riceve una chiave di produzione valida solo temporaneamente. Trasformazione in chiave impianto invisibile al primo utilizzo.
   --> Nessuna copia della scheda ID passa inosservata!
3. Schede ID sicure:
   ogni singola scheda ID è protetta da una chiave di accesso personalizzata e unica.
   --> In questo modo si evita il furto dei dati e non è possibile risalire alle informazioni di altre schede ID!
4. Funzionamento sicuro:
   i moduli di sicurezza in tutti i componenti proteggono le chiavi dati mediante meccanismi di crittografia riconosciuti.
   --> Nessuna chiave dati non protetta!

Tabella di 4.1: sicurezza degli impianti a confronto

	MIFARE Classic Standard	MIFARE Classic ARIOS-2
Tutte le schede hanno la stessa chiave delle applicazioni.	Caso più comune in ambito applicativo. I supporti possono essere copiati senza incorrere in grandi ostacoli.	Non utilizzato
Ogni scheda ha la propria chiave delle applicazioni.	Esistono fornitori di dispositivi MIFARE che dispongono di una protezione supplementare, simile a quella di ARIOS-2. Pertanto, è possibile copiare solo una scheda. La sicurezza dipende dall'applicazione.	Con ARIOS-2, ogni supporto dispone della propria chiave (Application Key). La sicurezza è ulteriormente aumentata, in quanto la Application Key dipende dall'UID della scheda utente.

4.4 Quali applicazioni supporti si basano sul concetto di sicurezza ARIOS-2?
I dati di accesso sono memorizzati in una struttura dati analogamente a LEGIC. La tabella sottostante mostra il confronto con i segmenti LEGIC noti.

4.5 Come si protegge ARIOS-2 dai vari tipi di attacchi?
I meccanismi sono descritti nei capitoli 4.2 e 4.3. Ulteriori dettagli si trovano nel White paper ARIOS-2.

4.6 Quanto è sicuro il funzionamento con l'UID?
Lo standard ISO 14443A non fornisce alcuna garanzia in termini di sicurezza per il funzionamento con UID. ARIOS-2 supporta il metodo „Save UID", grazie al quale, oltre all'UID viene letto un pacchetto di dati (KCA) [2] dal supporto. L'autorizzazione all'accesso è così determinata da una procedura criptata. Se viene simulato un UID senza KCA, il codice di accesso non può essere determinato.

4.7. È prevista la consegna di una chiave al produttore della scheda?
Al produttore della scheda viene rilasciata una chiave di fabbrica, la quale viene utilizzata solo per la produzione di schede. Se nell'impianto viene integrata una scheda, la chiave di fabbrica viene sostituita dalla chiave delle applicazioni. Questo processo viene controllato e protocollato dal sistema, in modo da rilevare qualsiasi duplicato creato dal produttore della scheda, in quanto questa conversione della chiave può essere effettuata solo una volta per una scheda utente con lo stesso UID.

Tabella di 4.4: struttura dati dormakaba ARIOS-2

Configurazione

Segmenti LEGIC	**MIFARE Classic ARIOS-2 file**	**MIFARE DESFire ARIOS-2 Applicazioni**
Kaba Group Header	File di identificazione	Applicazione di accesso
CardLink	CardLink Data CardLink Stato attuatore	CardLink Data CardLink Stato attuatore Traceback
LockerLock Selezione libera	LockerLock Selezione libera	LockerLock Selezione libera
Biometria		Applicazione biometrica

Non è incluso, ad esempio, il Cash-Segment, in quanto queste applicazioni sono fornite da fornitori terzi.

5. Supporti MIFARE

5.1 Quali supporti utente possono essere utilizzati?
Nell'impianto, si raccomanda di utilizzare supporti utente dello stesso tipo. Esistono diversi produttori. La distanza di lettura può variare da produttore a produttore, poiché i processi di produzione non sono standardizzati. Nel caso di MIFARE, si consiglia di utilizzare solo schede di produttori "certificati MIFARE".

5.2 Chi è in grado di codificare le schede?
Ogni produttore di schede può codificare le schede con la chiave di fabbrica.

5.3 Dove si può reperire la scheda?
In linea di principio, i supporti utente possono essere acquistati da qualsiasi fornitore di schede o presso dormakaba. dormakaba fornisce esclusivamente supporti con la tecnologia MIFARE DESFire consigliata.
Le tessere di sicurezza e i master di programmazione sono forniti esclusivamente da dormakaba.

5.4 È possibile cambiare il fornitore della scheda dopo la prima fornitura?
Sì.

In caso di cambiamento, al produttore della scheda devono essere fornite le seguenti informazioni:
- File AEF (formato XML) o Print Information (formato PDF), creato con Media Workstation (MWS)

5.5 È possibile utilizzare una scheda MIFARE Classic o DESFire già esistente?
Sì; come requisito fondamentale, deve essere nota la chiave di manutenzione dei supporti.

Si possono distinguere due casi:
1. l'applicazione ARIOS-2 deve essere applicata (terminale) al supporto esistente. A tal scopo, ci deve essere sufficiente spazio di memoria libero sul supporto.
2. deve essere possibile leggere il numero programmato esistente. A tal fine, è necessario conoscere la codifica del numero.

I dettagli devono essere chiariti con gli specialisti ARIOS-2.

Tabella di 5.1: quali supporti utente possono essere utilizzati con ARIOS-2?

Tipo di scheda	Dimensioni memoria [2]	Applicazioni di sistema supportate
MIFARE DESFire EV1/EV2	8kB consigliato 2kB e 4kB possibili	CardLink (KXA) Protetto da UID (KCA)
MIFARE Classic	1kB, 4kB	CardLink Protetto da UID (KCA)

[2] In un impianto si possono usare schede con diverse dimensioni di memoria.