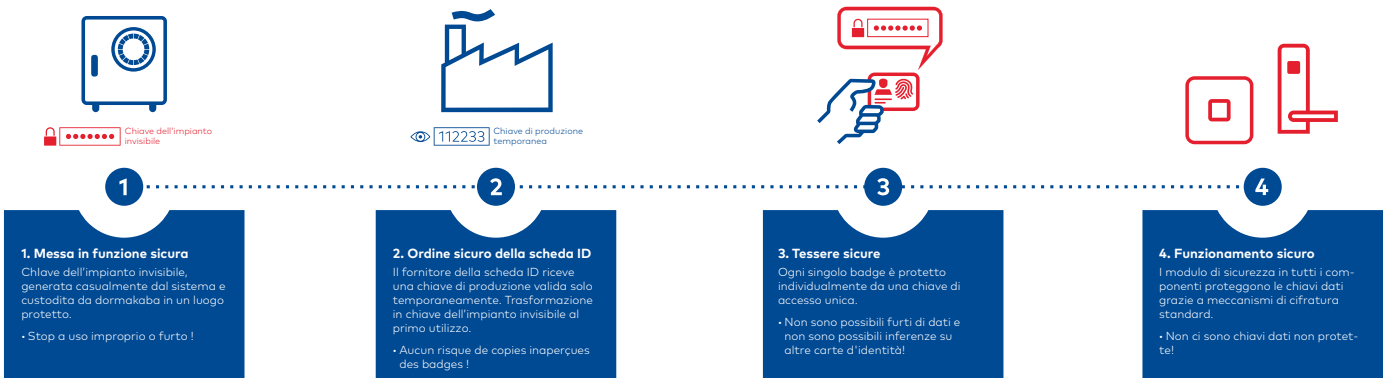
White paper: il concetto di sicurezza ARIOS-2 di dormakaba

Perché ARIOS-2 offre una maggiore sicurezza per 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 controllo degli accessi ancora più sicuro.

Un elemento fondamentale di ARIOS-2 è la chiave di sicurezza univoca, che viene generata tramite generatore casuale e non è visibile a nessuno, garantendo un elevato livello di sicurezza in tutte le fasi del processo: dalla generazione, alla messa in funzione, alla produzione di schede ID fino alla manutenzione. Ad esempio, al momento dell'ordine delle schede ID, per il produttore viene creato un codice specifico per ogni singolo impianto. Solo quando vengono consegnate le nuove schede ID, tale codice viene convertito nella chiave impianto in un processo sicuro di ARIOS-2. Tale processo viene protocollato nel sistema in modo che nessuna scheda ID prodotta illegalmente possa essere utilizzata passando inosservata.

Inoltre, lo scambio di dati tra il lettore e la scheda ID è criptato con le procedure riconosciute AES o 3DES, al fine di proteggere i gestori del sistema dagli scenari di hackeraggio attualmente diffusi, come i sistemi di reverse engineering o gli attacchi man-in-the-middle.
I meccanismi di sicurezza ARIOS-2 si estendono addirittura alla singola scheda ID, pertanto la crittografia dati è individuale per ognuna di esse. In tal modo, i malintenzionati non hanno alcuna possibilità di risalire alle informazioni sulla crittografia di un intero impianto.

Che cos'è ARIOS-2?

Il concetto di sicurezza ARIOS-2 risolve una vulnerabilità delle applicazioni RFID il cui meccanismo di sicurezza si basa su una chiave dati definita dall'utente.

In assenza di ARIOS-2, la chiave dati MIFARE può essere facilmente divulgata o spiata senza dare all'occhio. Il concetto di sicurezza ARIOS-2 aiuta gli utenti a memorizzare le loro chiavi dati in modo sicuro e semplice, evitando così la divulgazione o la manipolazione inavvertita e aumentando il livello di sicurezza del sistema.
Questo documento illustra i singoli meccanismi e gli elementi fondamentali del concetto di sicurezza, evidenziando quali vantaggi gli utenti ARIOS-2 possono ottenere in termini di sicurezza per la loro soluzione di controllo degli accessi.

dormakaba

dormakaba ARIOS-2 – Concetto di sicurezza
Elementi fondamentali

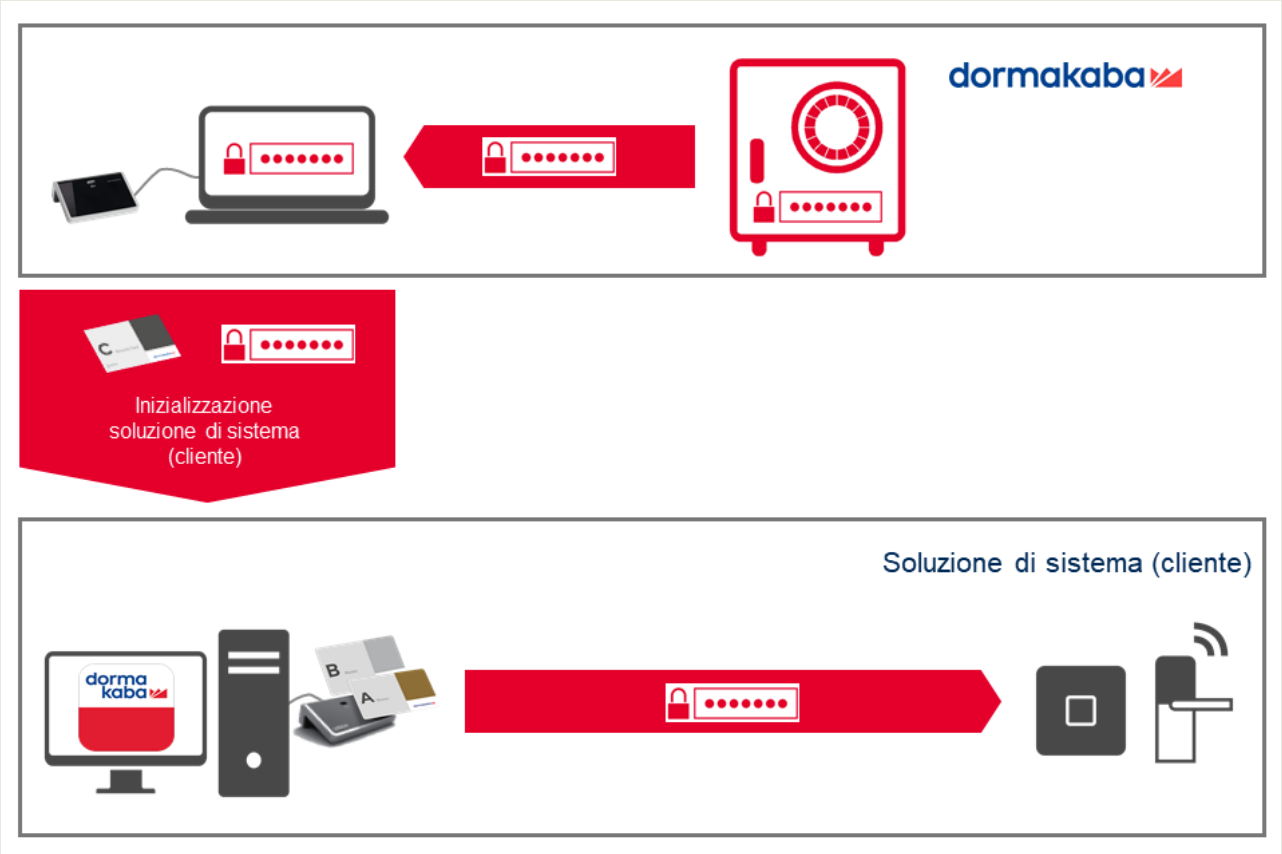
1. Chiave impianto

L'elemento centrale del concetto di sicurezza di ARIOS-2 è la chiave impianto. Il concetto ARIOS-2 assicura che la chiave impianto non divenga mai nota. La chiave impianto, specifica per il cliente, segreta e invisibile, viene generata e conservata in modo sicuro in un ambiente dormakaba appositamente protetto.

Con ARIOS-2, grazie alla chiave impianto è possibile far funzionare diversi impianti in modo completamente indipendente l'uno dall'altro.

Inoltre, ARIOS-2 offre una sicurezza supplementare, in quanto la chiave impianto non viene utilizzata per autorizzare direttamente un supporto utente, come è altrimenti usuale nelle applicazioni MIFARE. In ARIOS-2, la chiave impianto fornisce la base di calcolo per determinare la chiave di accesso individuale per un supporto utente.

Chiave impianto e supporti di autorizzazione: mai visibili e mai leggibili!



2. Supporti di autorizzazione (supporti master)

Dopo la generazione, la chiave impianto viene portata all'impianto su un supporto di autorizzazione. I supporti di autorizzazione consentono al proprietario di mettere in funzione l'impianto e di apportare modifiche. Il grande vantaggio di un tale supporto è che può essere utilizzato in modo controllato in qualunque momento, evitando qualsiasi comunicazione orale e scritta. Il concetto si basa quindi sul "possesso" e non sulla "conoscenza" (segreto condiviso).

Il concetto di sicurezza di ARIOS-2 utilizza due tipi di supporti di autorizzazione:
- tessera di sicurezza
- master di programmazione (tipo A/tipo B)

2.1. Tessera di sicurezza C

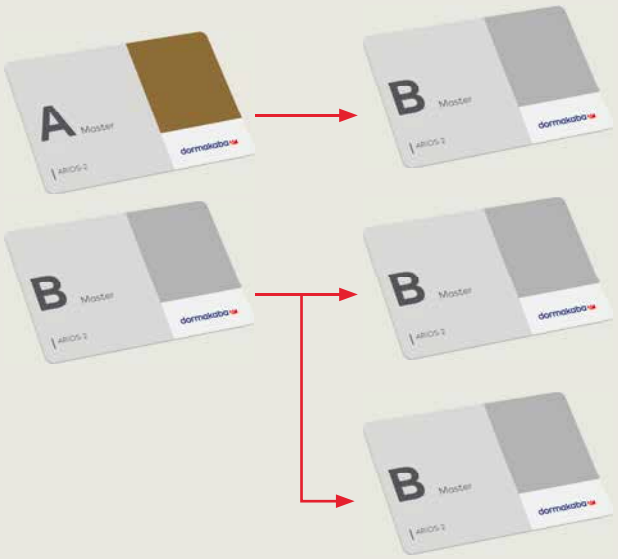
La tessera di sicurezza C è una scheda ID di tipo RFID per l'inizializzazione dell'applicazione di sistema e deve quindi essere conservata in un luogo sicuro dopo l'uso. La tessera di sicurezza C è fornita da dormakaba ed è del tipo MIFARE DESFire. I dati rilevanti per la sicurezza, come la chiave impianto e i dati di configurazione, vengono memorizzati sulla tessera di sicurezza C in forma criptata (3DES o AES). Per utilizzare la tessera di sicurezza C è necessario il lettore da tavolo dormakaba. Durante la messa in funzione, la chiave impianto crittografata con 3DES o AES viene trasferita dalla tessera di sicurezza o dal master di programmazione a tutti i componenti del sistema e memorizzata. La chiave impianto non è mai visibile. Il trasferimento sui componenti stand-alone avviene manualmente (in loco) con il master di programmazione, mentre sui componenti online avviene attraverso l'infrastruttura di sistema (centralmente).

2.2 Master di programmazione A/B

I master di programmazione sono schede ID di tipo RFID con le quali vengono inizializzati, mantenuti e programmati i componenti stand-alone. Per ragioni amministrative, i contenuti possono essere ereditati da altri master di programmazione (non ci sono duplicati). I master di programmazione sono forniti da dormakaba e sono del tipo MIFARE DESFire. I dati rilevanti per la sicurezza, come la chiave impianto, vengono memorizzati in forma criptata (3DES o AES) sul master di programmazione. Per l'utilizzo, è necessario il lettore da tavolo dormakaba.

Tessera di sicurezza C

Master di programmazione A



Panoramica dei supporti di autorizzazione

	Tessere di sicurezza	Master di programmazione
Tipi	Tipo C	Tipo A/Tipo B
Funzioni	Inizializzazione delle applicazioni di sistema (disponibile almeno una volta per impianto)	Inizializzazione di componenti stand-alone
Possibilità di creare copie	No	No (è possibile un'ereditarietà limitata)
Supporto	MIFARE DESFire (contactless)	MIFARE DESFire (contactless)
Contenuto dei dati	– Copia crittografata dei dati di sicurezza di ARIOS-2 – Dati di configurazione dell'impianto	Copia crittografata dei dati di sicurezza di ARIOS-2

3. Chip di sicurezza nel lettore da tavolo

Il lettore da tavolo 91 08 MRD è un componente importante nella configurazione della soluzione di accesso. Durante la configurazione, la tessera di sicurezza C deve essere rispettivamente collocata sul lettore da tavolo e letta. Se l'applicazione di sistema o il computer della postazione di lavoro viene spento, i dati di sicurezza nel lettore da tavolo vengono nuovamente persi.
Le applicazioni di sistema con una propria autorizzazione utente (ad es. Kaba exos 9300) sono in grado di memorizzare i dati della tessera di sicurezza anche nella banca dati del sistema.

Dopo aver avviato il lettore da tavolo inizializzato, i dati di sicurezza vengono nuovamente caricati. Quindi, la tessera di sicurezza deve essere inserita solo una volta quando il lettore da tavolo viene messo in funzione, poiché i dati di sicurezza sono crittografati anche nell'applicazione di sistema (3DES). Questa funzione agevole consente di lavorare in modo efficiente senza vulnerabilità. Se il lettore da tavolo viene sottratto (ossia se viene scollegato dall' applicazione di sistema) perde tutti i dati. Nel funzionamento normale, questo lettore viene utilizzato per l'emissione e l'acquisizione dei supporti.

dormakaba ARIOS-2
Meccanismi di accesso e di crittografia

La generazione automatica della chiave impianto garantisce che essa non divenga mai nota in nessun caso. Nell'improbabile eventualità che la chiave impianto di un qualsiasi impianto venga violata, solo quello interessato sarebbe a rischio grazie alla struttura di autorizzazione orizzontale che non permette di risalire ai dati di un altro impianto. La sicurezza verrebbe ripristinata generando una nuova chiave per l'impianto in questione. Per assegnare una chiave impianto e accedere ai supporti utente viene utilizzata una crittografia 3DES o AES128. I meccanismi crittografici utilizzati possono essere messi a disposizione dei gestori di sistema interessati in qualsiasi momento.

Chiave impianto
La chiave impianto viene generata con un generatore casuale certificato.

Chiave delle applicazioni
La chiave delle applicazioni viene utilizzata per accedere (autenticare l'accesso) ai dati nel supporto utente. Per motivi di sicurezza, ogni applicazione su ogni singolo supporto utente ha la propria chiave delle applicazioni.

Grazie a questo metodo, si ottiene un elevato livello di sicurezza. Nel caso una chiave delle applicazioni venisse decodificata, solo l'applicazione sul supporto utente interessato sarebbe compromessa. Non sarebbe possibile risalire alle informazioni di altri supporti utente.

La codifica della chiave delle applicazioni è strutturata come segue:
- chiave impianto dell'applicazione
- numero unico del supporto utente
- identificativo della rispettiva applicazione supporti

Composizione della chiave delle applicazioni

Chiave lettura dei supporti
Questa chiave consente a un sistema o dispositivo di terze parti, che non supporta il concetto ARIOS-2, di leggere il numero di identificazione programmato sul supporto utente. Oltre a questa chiave lettura dei supporti, al gestore vengono trasmessi altri dati strutturali in modo che il numero possa essere letto e interpretato correttamente.

Chiave delle applicazioni di terze parti
La chiave delle applicazioni di terze parti assicura la migrazione durante il funzionamento. Per continuare a utilizzare i supporti utente esistenti di fornitori terzi, ARIOS-2 supporta il seguente caso d'uso:

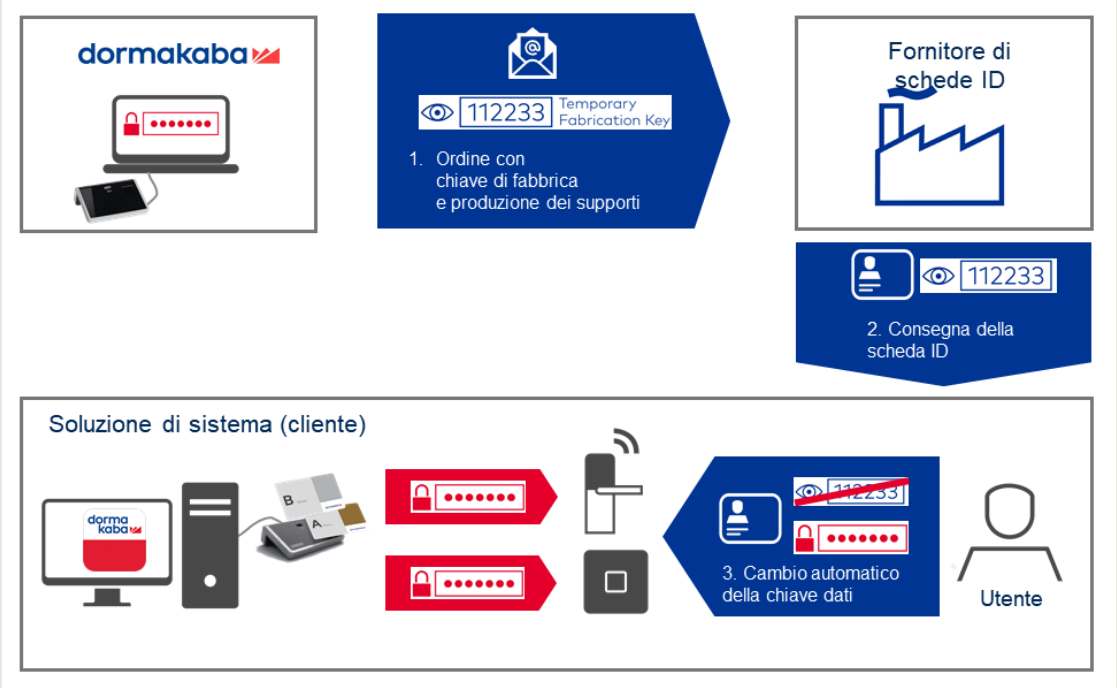
- lettura del numero di identificazione dell'applicazione di terze parti.
  In questo caso, i supporti di autorizzazione ARIOS-2 dell'impianto vengono ampliati con l'applicazione di terze parti. La chiave delle applicazioni di terze parti occupa lo stesso spazio di memoria di una chiave impianto.

Per la migrazione di schede ID esistenti di terze parti, il seguente caso d'uso è possibile anche senza chiave delle applicazioni di terze parti:

- lettura del numero di identificazione:
  per leggere il numero di identificazione ARIOS-2, ai supporti utente dev'essere aggiunta l'applicazione ARIOS-2.

Chiave di fabbrica
Nel mondo MIFARE, la creazione di supporti utente rappresenta una vera sfida in termini sicurezza. Di solito, al produttore della scheda viene fornita una definizione dei supporti utente desiderati (tipi di scheda ID) nonché la chiave segreta. Questo implica un atto di fiducia nei confronti del produttore della scheda, in quanto non è possibile alcun controllo. Grazie alla chiave di fabbrica, questa vulnerabilità viene eliminata, in quanto tale chiave viene generata per derivazione dalla chiave impianto sia per il file (Classic) sia per l'applicazione (DESFire) e non può essere ricalcolata. La chiave di fabbrica viene consegnata al produttore con l'ordine di produzione. Se il supporto utente viene utilizzato per la prima volta sull'applicazione di sistema, quest'ultima riconosce la chiave di fabbrica e la sostituisce con la chiave delle applicazioni, che è univoca per ogni supporto utente e per ogni file/applicazione. Se un produttore di supporti dovesse produrre la stessa identificazione due volte, essa verrebbe rilevata e tutti i supporti con questa ID verrebbero immediatamente bloccati.

Creazione sicura dei supporti e inizializzazione dei supporti tramite chiave di fabbrica



Avete altre domande? Saremo lieti di offrirvi la nostra consulenza.

dormakaba Italia S.r.l. | IT-Milano (MI) · T +39 02 494842 | IT-Castel Maggiore (BO) · T +39 051 4178311 | info.it@dormakaba.com | www.dormakaba.it
dormakaba Schweiz AG | Mühlebühlstrasse 23 | CH-8620 Wetzikon | T +41 848 85 86 87 | info.ch@dormakaba.com | www.dormakaba.ch

MIFARE è un marchio registrato di NXP B.V
Con riserva di modifiche tecniche. © 2020 dormakaba. 06/2020