RKD32 Sistema di Gestione chiavi - Guida Installazione

Versione 1.0, Agosto 2024

DOINGPRO SRL, ING. GIANNI SABATO
Registered office: Via E. Fermi 25, I-40033 Casalecchio di Reno (BO)
Operational HQ: Via F. Baracca 7, I-40033 Casalecchio di Reno (BO)
GSM +39 335 238046
Ph. +39 051 6211553
E-mail: info@doingsecurity.it
Web: www.doingsecurity.it

Assistenza tecnica Tel.: +39 335 238046 / +39 051 6211553

Tel.: +39 329 2288344 email: info@doingsecurity.it

Indice

1 Introduzione

Il presente documento illustra come installare e utilizzare il sistema di gestione delle chiavi RKD32.

RKD32 è un pannello in cui ciascuna chiave è permanentemente collegata ad un key-fob dotato di chip RFID a sua volta inserito in uno slot del pannello che ne blocca meccanicamente l'estrazione, se non autorizzata. L'estrazione di una chiave può avvenire solo da parte di un utente autorizzato e in funzione di specifici limiti di autorizzazione, per esempio su base temporale. È previsto un sistema di prenotazione delle chiavi e un reporting sull'uso del sistema da parte degli utenti.

RKD32 è gestito dal terminale MD70 con touch-screen e lettore RFID (compatibile Mifare® e EM 125 kHz) in grado di gestire fino a 6 pannelli con 32 slot-chiave ciascuno. L'utente può identificarsi sul terminale in modalità PIN, Prox oppure PIN & Prox; se richiesto, l'utente può identificarsi mediante un lettore esterno collegato in Wiegand o su bus RS485 (in quest'ultimo caso il lettore deve essere di marca Roger).

RKD32 può essere utilizzato in modalità stand-alone oppure in rete locale via browser mediante un software fornito in licenza. Un SDK è disponibile su richiesta per i system integrators.

Il Manuale descrive le diverse operazioni di posa del pannello RKD32 e le operazioni di programmazione e gestione attraverso il touchscreen e il lettore RFID.

Immagini e fotografie o altre informazioni di carattere grafico sono inseriti nel Manuale esclusivamente a titolo descrittivo ed esplicativo. Si rammenta che le informazioni contenute nel presente Manuale sono soggette a modifiche, senza preavviso, a fronte di aggiornamenti del firmware/software o per altri motivi.

Salvo disposizioni contrarie, DOINGSECURITY non rilascia alcuna garanzia, assicurazione o dichiarazione, esplicita o implicita, in merito al presente Manuale.

Entro i limiti previsti dalla Legge in vigore, il prodotto - completo di hardware, software e firmware - viene fornito "così com'è" compresi gli eventuali difetti e gli errori: DOINGSECURITY Sas non fornisce alcuna garanzia, esplicita o implicita, incluse, senza limitazione, garanzia di commerciabilità, di qualità soddisfacente, di idoneità per uno scopo particolare e di non violazione di diritti di terzi. In nessun caso DOINGSECURITY Sas, i suoi Dirigenti, Funzionari, Dipendenti o Agenti saranno responsabili per eventuali danni speciali, consequenziali, incidentali o indiretti, compresi, tra gli altri, danni per perdita di profitti, interruzione dell'attività o perdita di dati o di documentazione connessi all'uso di questo prodotto, anche qualora DOINGSECURITY Sas fosse stata informata della possibilità del verificarsi di tali danni. L'utente si assume interamente ogni rischio correlato dall'utilizzo del prodotto con accesso Internet: DOINGSECURITY

Sas declina ogni responsabilità per anomalie di funzionamento, perdita di privacy o altri danni derivanti da un attacco cibernetico, attacco da parte di hacker, virus o altri rischi e minacce alla sicurezza, correlati all'utilizzo di Internet. Tuttavia DOINGSECURITY Sas fornirà supporto tecnico tempestivo, se necessario.

Considerata la variabilità di normativa applicabile, si prega di controllare tutte le Leggi pertinenti e vigenti nella propria giurisdizione prima di utilizzare questo prodotto, al fine di garantire che l'utilizzo sia conforme alle Leggi vigenti: DOINGSECURITY Sas declina ogni responsabilità nel caso in cui questo prodotto venga utilizzato per scopi illeciti. In caso di eventuali conflitti tra il presente Manuale e la Legge applicabile, prevale quest'ultima.

1.1 Utilizzo del prodotto

Per il corretto utilizzo del sistema, seguire le istruzioni riportate di seguito:

- Controllare il contenuto della confezione - compresi gli accessori di montaggio
- Per alimentare il pannello RKD32, usare una linea di alimentazione 230 Vca, 50 Hz, proveniente da un quadro elettrico con differenziale e sezionatore adeguati
- Leggere attentamente le presenti istruzioni di montaggio e utilizzo
- Assicurare che l'installazione sia eseguita da un tecnico qualificato, nel rispetto di tutte le normative locali
- Se il prodotto risultasse non funzionante in modo corretto, contattare il produttore ai numeri riportati all'inizio del documento.

Il pannello RKD32 - espandibile e modulare - è illustrato in Fig. 1.1.

Fig. 1.1. *RKD32 con espansioni*

1.2 Specifiche tecniche RKD32

Le principali caratteristiche e prestazioni del pannello RKD32 sono elencate nella tabella sottostante.

☐ Prestazione	Descrizione
Operatività	Stand-alone o in rete con software opzionale
Terminale di controllo	Touch-screen 7” Lettore Mifare® 13,56 MHz e EM 125 kHz Supporto per la gestione dei settori Secure Mifare® Interfaccia Wiegand per identificazione su lettore esterno di terze-parti Interfaccia RS485 per identificazione su lettore esterno Roger One Time PIN Foto utente al momento del prelievo / restituzione chiave
Modularità	32 chiavi nel pannello principale; 32 o 24 chiavi nei pannelli di espansione Massimo 5 pannelli di espansione per ciacun RKD32 master
Keyfob	Collegato alla chiave in modo permanente, tecnologia RFID Mifare® Controllo della presenza del keyfob nello slot occupato Posizione dei keyfob fissa o variabile Illuminazione con Led verde dello slot con la chiave selezionata
Opzioni di autorizzazione utente	Su base tempo; doppio-utente; PIN & Prox
Allerte	Segnalazione se la chiave non viene restituita entro un tempo predefinito
Notifiche	Notifica email ad ogni evento di allarme
Prenotazione chiave	Funzione prevista nel terminale di controllo
Report	Attività Utente / Utilizzo Chiave
Avvisi vocali	Prompt vocali
Emergenza	Sblocco di tutte le chiavi in caso un segnale digitale esterno sia attivo
Meccanica	Cabinet metallico, colore RAL7016 Dimensioni modulo Master: 600 (A) x 969 (L) x 183 (P) mm., peso 39 kg Dimensioni modulo di Espansione: 600 (A) x 677 (L) x 183 (P) mm., peso 29,5 kg Opzione SG: vetro frontale anti-vandalismo, classe P2 Uso in interno
Alimentazione	230 Vca, spazio per batteria 17 Ah. Consumo 2A
Condizioni ambientali di uso	Class I, IP41. Temperatura da +5°C a +40°C, U.R. < 95% senza condensa

1.3 Avvertenze

Tener presente che i prodotti descritti nel presente documento e i relativi accessori, ove applicabile, sono marchiati “CE” e sono conformi alle seguenti direttive:

- Direttiva 2014/35/EU (Low Voltage - N.A.)
- Direttiva 2014/30/EU (EMC)
- Direttiva 2014/53/EU (RED)
- Direttiva 2011/65/EU (RoHS)
- Direttiva 2006/1907 (REACH)

Tener presente la direttiva 2012/19/EU (WEEE): il prodotto, a fine vita, è soggetto a procedura di riciclo rifiuto come da normativa. Il prodotto va reso al fornitore a fronte di acquisto di un nuovo apparato o portato in rifiuteria agli appositi punti di raccolta.

1.4 Terminologia

- **Ethernet -** tecnologia di comunicazione per la realizzazione di reti di computer in ambito locale (LAN)
- **LAN -** rete locale, rete di computer per un'area di piccole dimensioni, per es. un ufficio, un'abitazione o un gruppo di edifici come una scuola o un aeroporto
- **10Base-T -** 10 Mbit/s, usa un connettore modulare a 8 vie, generalmente chiamato RJ45, nell'ambito Ethernet con coppie twistate. I cavi generalmente usati sono a 4 coppie twistate (sebbene 10BASE-T e 100BASE-TX usino solamnete due di tali coppie). Ciascun stardard supporta la comunicazione sia full-duplex che half-duplex. Operano su distanze fino a 100 metri
- **100Base-TX -** noto come **Fast Ethernet**, usa due coppie UTP o STP, CAT5
- **Coppia Twistata -** è un cablaggio nel quale due conduttori sono twistati insieme per cancellare l'interferenza elettromagnetica (EMI) proveniente da sorgenti esterne, per esempio la radiazione elettromagnetica da cavi non schermati, e il crosstalk da coppie poste nelle vicinanze
- **UTP**, Unshielded Twisted Pair - coppia twistata non schermata
- **STP**, Shielded Twisted Pair - coppia twistata schermata; uno schermo metallico è posto attorno a ciascuna coppia per proteggere il cavo da interferenze elettromagnetiche (EMI)
- **WEB -** World Wide Web (WWW), applicazione del protocollo internet HTTP
- **HTTP -** Hypertext Transfer Protocol; è un protocollo internet usato originariamente per lo scambio di documenti ipertestuali in formato HTML
- **USB -** Universal Serial Bus; metodo per la connessione seriale di dispositivi esterni al computer
- **Video codec** - compressione **H.263** derivata da MPEG-4, **H.264** è un codec per il formato AVC MPEG-4. **MPEG-4** è un tipo di compressione video
- **JPEG** è un metodo standard di compressione usato per salvare immagini digitali
- **Voice over Internet Protocol** (**VoIP**) è una tecnologia che permette la trasmissione di voce digitalizzata all'interno di paccetti del protocollo **UDP/TCP/IP** nelle reti di computer. È usato per effettuare telefonate via Inernet, Intranet o altri tipologie di connessioni dati
- **TCP/IP** contiene un set di protocolli per la comunicazione nelle reti di computered è il protocollo principale di Internet
- **IP address** è un numero che identifica chiaramente una interfaccia nella rete di computer che usa il protocollo IP

- **DHCP** (Dynamic Host Configuration Protocol) è un protocollo della famiglia TCP/IP. È usato per assegnare automaticamente indirizzi IP a singoli PC nelle reti di computer, semplificando il lavoro dell'amministratore di rete
- **Internet** è un sistema di reti di computer connessi a livello mondiale
- **Intranet** è una rete di computer simile a Internet, ma di tipo privato. Questo significa che è usata esclusivamente da un gruppo di utenti limitato (es. Una azienda e le sue filiali)
- **PoE** (Power over Ethernet) è un sistema di alimentazione attraverso il cavo di rete che non necessita di ulteriori cablaggi per la fornitura di energia elettrica
- **NTP** (Network Time Protocol) è un protocollo per la sincronzzazione degli orologi interni ai computer
- **DTMF** (dual tone multi frequency) è il segnale del fornitore di servizio telefonico che è generato quando si preme un tasto di un normale telefono

2 Installazione

RKD32 e la chiave con key-fob sono mostrati in Fig. 2.1.

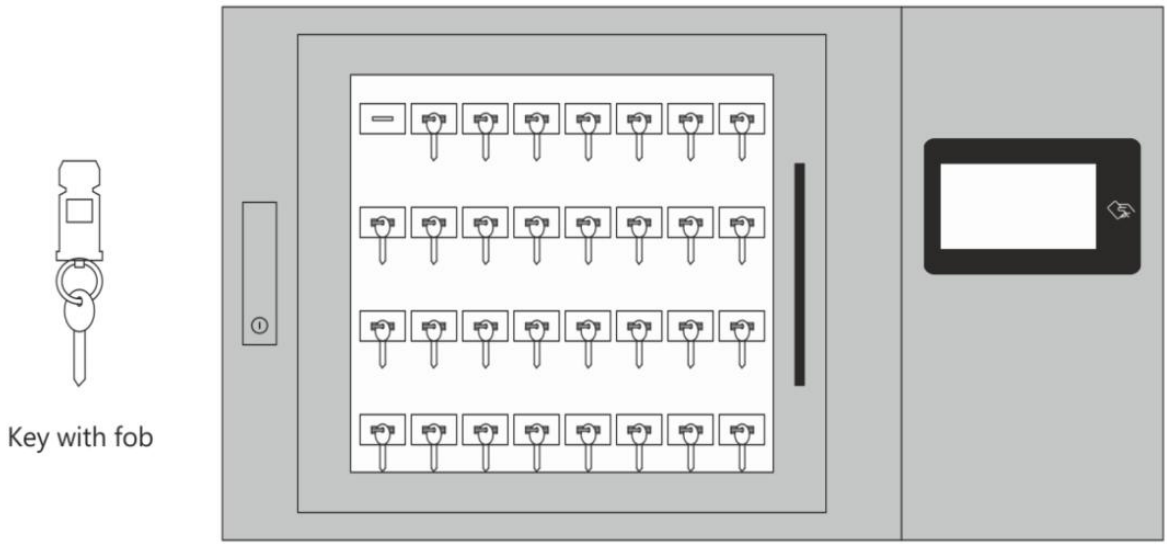

Fig. 2.1. *RKD32 e key-fob*

2.1 Connessione all'alimentazione

RKD32 è fornito con alimentatore 230Vca, 50 Hz e spazio per una batteria di back-up. Per collegare l'alimentazione, svitare il pannello e cablare i conduttori provenienti dal quadro elettrico.

NOTA.

Tutte le connessioni devono essere fatte in assenza di alimentazione elettrica. È vietato connettere più di una batteria.

In caso di mancanza di alimentazione, tutti i key-fob possono essere sbloccati in emergenza usando un powerbank con corrente di uscita minimo 2A collegato alla porta USB: lo sblocco della porta frontale e delle chiavi avviene come descritto nel par. 5.7 e deve essere effettuato individualmente per ciascun pannello, sia Master che Espansione.

2.2 Cabinet

RKD32 è fornito con porta frontale in vetro temperato. In opzione (SG) può essere dotato di vetro anti-sfondamento di classe P2; sempre in opzione è anche possibile avere una serranda motorizzata frontale. Le dimensioni sono mostrate in Fig. 2.2.

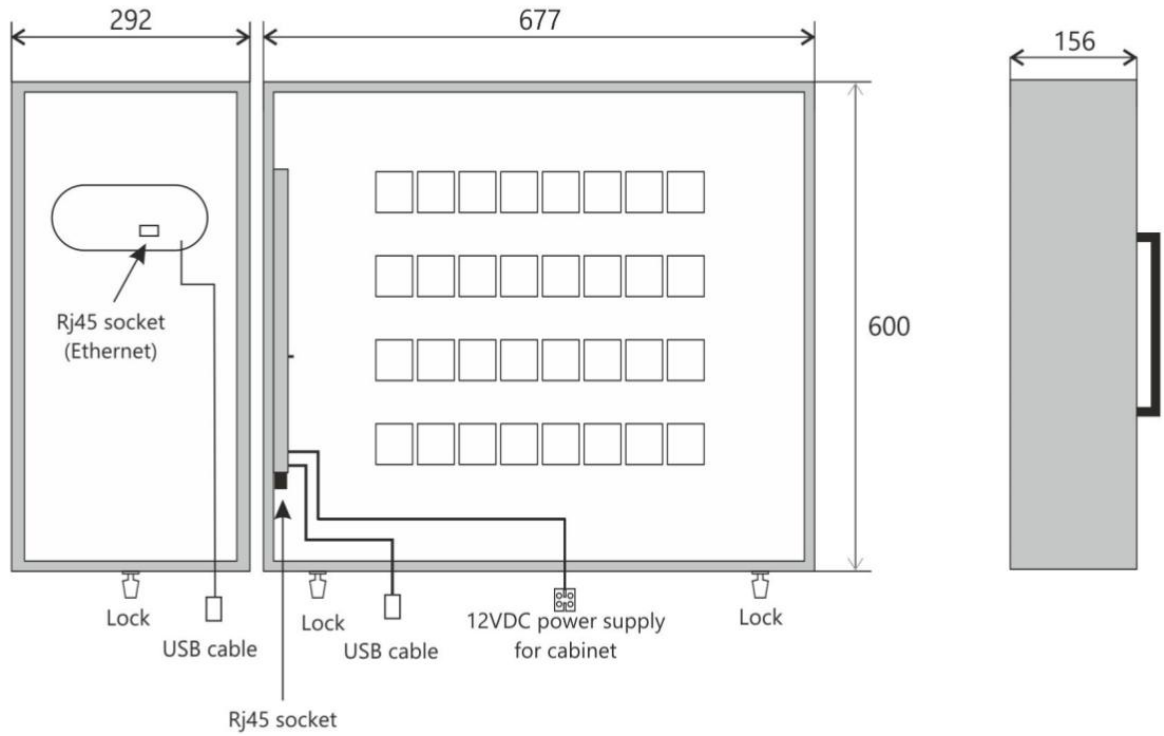

Fig. 2.2. *Pannello RKD32 e posizione delle interfacce*

2.3 Key-fob

RKD32 include 32 keyfob ai quali collegare altrettante chiavi. Il collegamento fra la chiave e il key-fob non richiede alcun strumento specifico: una volta che la chiave sia inserita nell'anello porta-chiave, l'anello viene inserito nel key-fob in modo che non possa essere più estratto a meno di danneggiarlo. Questo previene la possibilità di generare mix incontrollati di chiavi e key-fob.

L'anella con la chiave viene premuta nel key-fob finché non rimane visibile solo la parte ovale. Dopo l'inserimento verificare che l'accoppiamento chiave / key-fob permetta una corretta tenuta. Non è necessario utilizzare alcun sigillante ulteriore.

L'accoppiamento fra chiave e keyfob è mostrato nella Fig. 2.3.

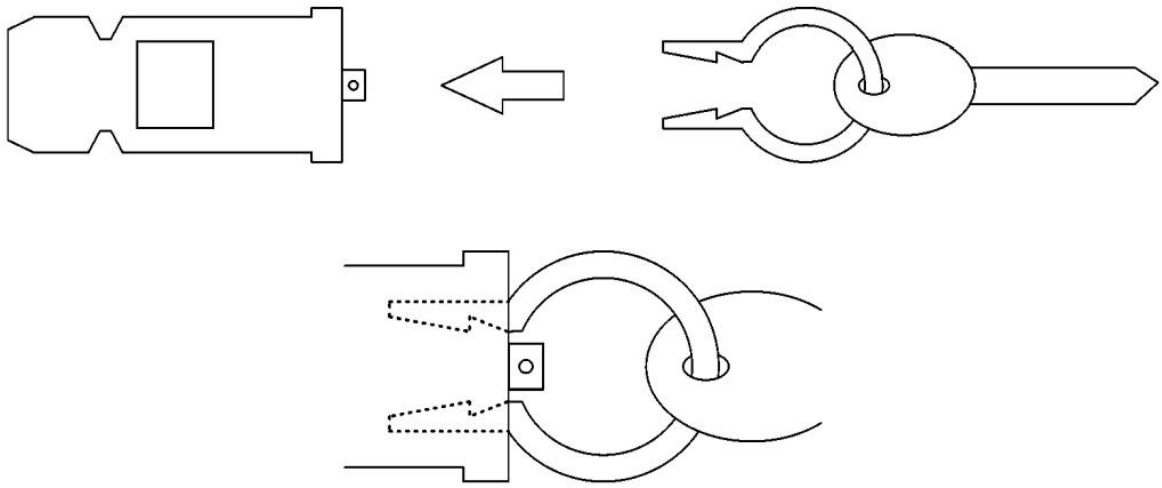

Fig. 2.3. *Accoppiamento chiave / keyfob*

2.4 Terminale di controllo

La gestione del pannello RKD32 è realizzata mediante un terminale MD70 con touch-screen grafico da 7" e un lettore RFID.

Il lettore RFID è compatibile con i seguenti standard:

- Mifare® Ultralight / Classic / Plus / DESFire
- EM 125 kHz

Per default il terminale legge il numero seriale delle tessere Mifare (CSN) ma è possibile programmare le tessere con il proprio numero (PCN) in settori criptati della memoria della tessera. L'uso dei PCN previene la clonazione non-autorizzata di carte e incrementa significativamente la sicurezza del sistema.

Se richiesto è possibile limitare l'identificazione di lettura RFID ad uno solo dei due standard, Mifare® o EM 125 kHz.

Il terminale legge PIN di lunghezza variabile (da 4 fino a 16 cifre). Il PIN una volta immesso con la tastiera touch deve essere terminato con il tasto # o il pulsante "Ok".

Se RKD32 viene programmato con la modalità "*Quick key return mode*", allora il key-fob collegato alla chiave può essere usato come identificativo sul lettore del terminale MD70 così da aprire la porta del RKD32 e inserire il keyfob in uno slot libero.

L'orientamento di lettura del key-fob sul lettore è mostrato in Fig. 2.4.

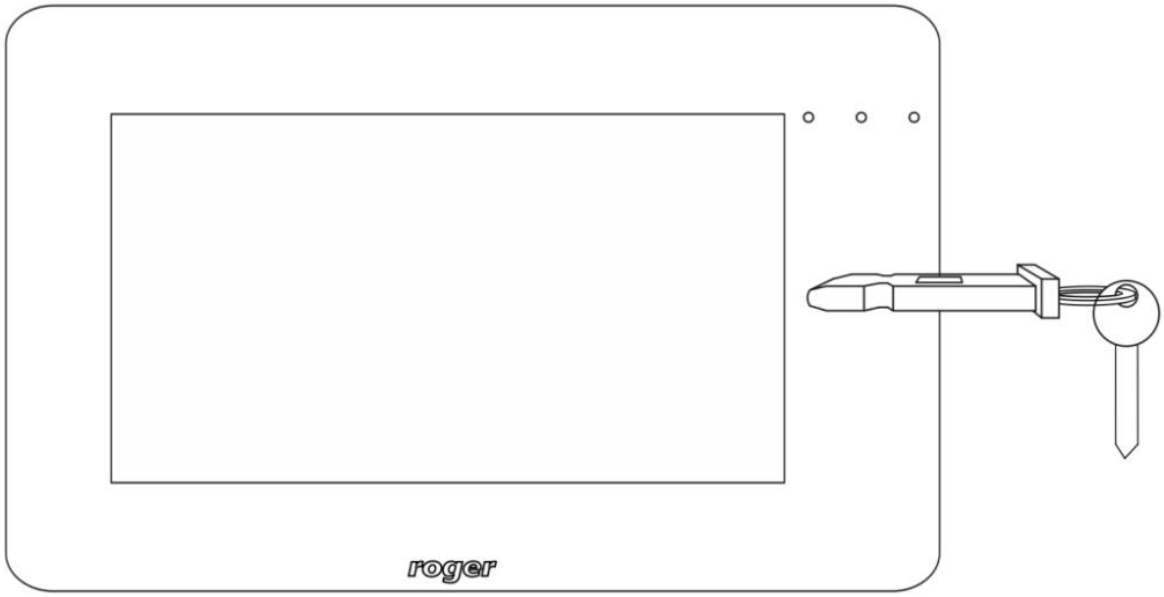

Fig. 2.4. *Orientamento di lettura keyfob sul terminale di controllo MD70*

NOTA.

Collegando un lettore esterno al terminale mediante l'interfaccia Wiegand, è possibile effettuare l'identificazione dell'utente con credenziali biometriche.

2.5 Collegamento con impianti di allarme

RKD32 è provvisto di tamper che rileva l'apertura porta del cabinet in modalità forzata. Un rilevatore tamper addizionale è posto all'interno del terminale di controllo.

Entrambi questi eventi sono segnalati mediante l'output a transistor LCK4 (15Vcc@1A).

L'avviso "Porta aperta troppo a lungo" è generato in modo acustico se il tempo trascorso fra l'identificazione utente e la richiusura del pannello eccede il parametro di preallarme: questo valore è di default 60 secondi. In caso di preallarme "Porta aperta troppo a lungo" viene attivato l'output BELL4 per 3 minuti che può essere collegato a impianti di allarme, sirene o altri dispositivi di allarme. Il medesimo output (15Vcc@1A) viene anche attivato istantaneamente in caso di porta forzata.

In caso di emergenza (per esempio un'evacuazione generata dal sistema anti-incendio), RKD32 può sbloccare tutte le chiavi e la porta frontale senza autorizzazione utente. Il segnale digitale proveniente dall'impianto anti-incendio deve essere cablato all'ingresso DR3 del terminale. L'opzione "*Fobs released*" deve essere abilitata per questa funzione.

2.6 Posa del pannello

È richiesta la presenza di almeno due persone per la posa del pannello RKD32. Sbloccare simultaneamente i LOCK mostrati in Fig. 2.2 così da staccare la parete metallica retrostante (Fig.2.5). Collegare il cavo 230Vca con l'alimentatore posto in un vano protetto con chiusura a viti usando i morsetti previsti. È presente anche un vano per una batteria da collegare usando i cavi inclusi nella confezione.

Fra i cabinet con le chiavi e il terminale di controllo devono essere seguite queste indicazioni:

- Cavo di alimentazione 12V da min 1 mm^2 connettendo i terminali 12Vcc e GND
- Cavo di rete RJ45, categoria 5E senza schermo per connettere i pannelli RKD32 1-6 (Master e 5 espansioni) di lunghezza max 5 m
- Per RKD32 master, collegare il cavo USB dal vano del terminale di controllo fino al cabinet con le chiavi.

Dopo aver eseguito le connessioni, attaccare RKD32 sulla parete del retro montata a muro come mostrato in Fig. 2.6. Infine bloccare i LOCK nelle posizioni mostrate in Fig. 2.2.

NOTA.

Il collegamento Ethernet alla porta RJ45 del terminale MD70 è richiesto solo se la gestione del pannello RKD32 è eseguita via browser e non in modalità stand-alone. Connettere il plug verde al socket Ethernet del terminale MD70 presente nel CONNECTION PANEL - vd. Fig. 2.7.

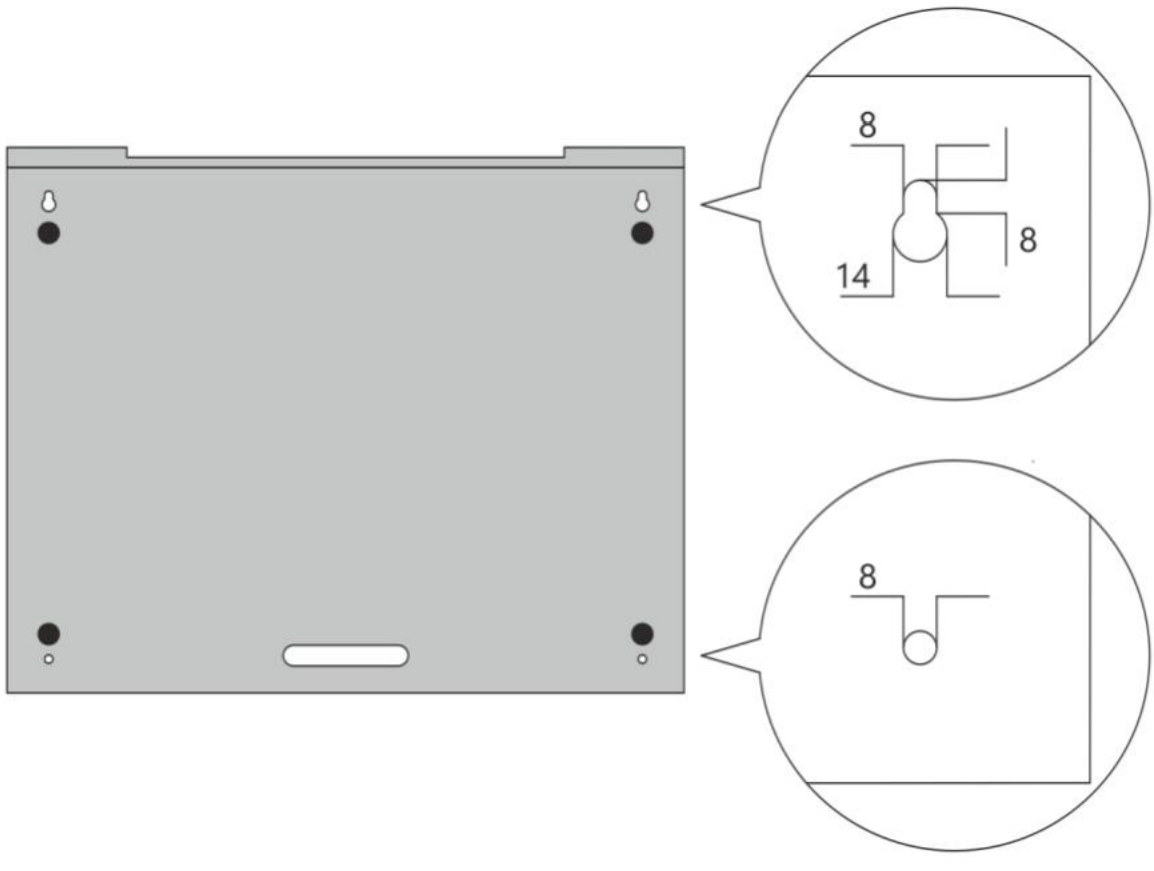

Fig. 2.5. *Parete retrostante*

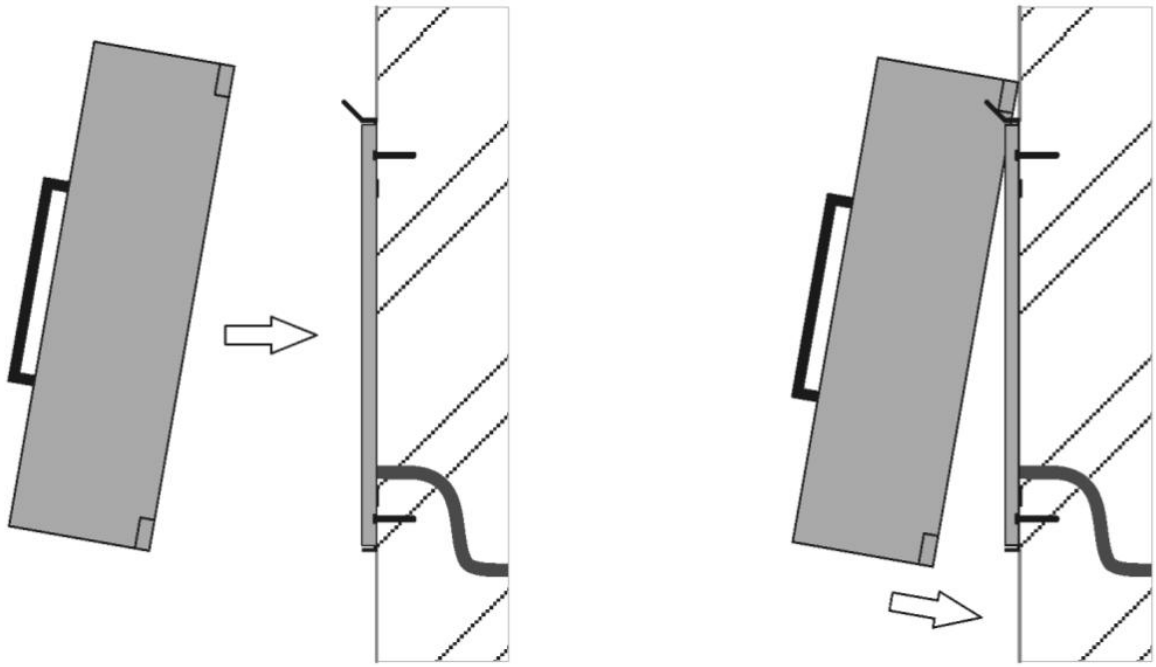

Fig. 2.6. *Montaggio a parete*

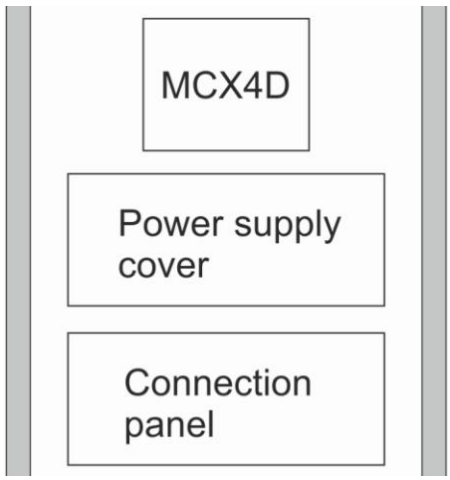

Fig. 2.7. *Posizione Connection Panel*

In caso di posa di RKD32EXT (espansioni del modulo RKD32 master) far riferimento alle Fig. 2.8 a) e 2.8 b).

Se l'aggiunta di RKD32EXT avviene successivamente alla posa del modulo master, avviare la funzione di "scansione dispositivi" dopo avere eseguito l'accesso con credenziali di amministratore nel menu "*Settings / Configuration / Detect devices*". Gli RKD32EXT devono essere per prima cosa collegati con cavo RJ45 al "Connection module" prima di fornire alimentazione.

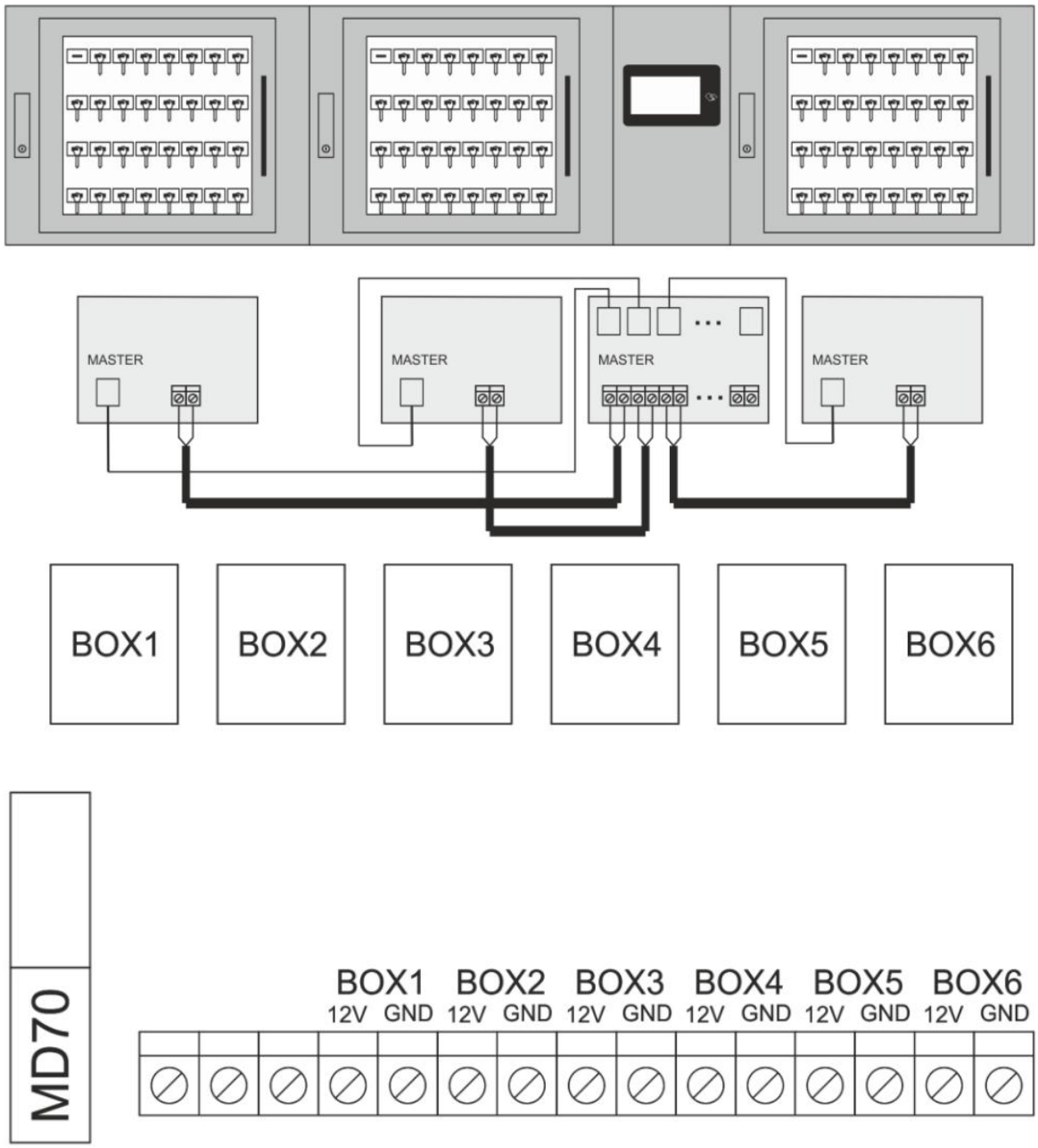

Fig. 2.8. *Collegamento RKD32 Master con le espansioni a) e b)*

Nella tabella sotto riportata sono indicati i significati dei diversi morsetti.

MORSETTO / SOCKET	SIGNIFICATO
+12V	Alimentazione 12Vcc
GND	Ground
BELL4	Linea output 15Vcc@1A di allarme porta
LCK3	Linea output 15Vcc@1A di allarme tamper
DR3	Linea input per sblocco chiavi
MASTER	Socket RJ45 per la comunicazione Master / Espansioni

Il socket USB per connettere memorie PenDrive (per effettuare backup o salvataggi di report) è disponibile in basso a destra nel RKD32 master dopo aver aperto la porta - vd. Fig. 2.9.

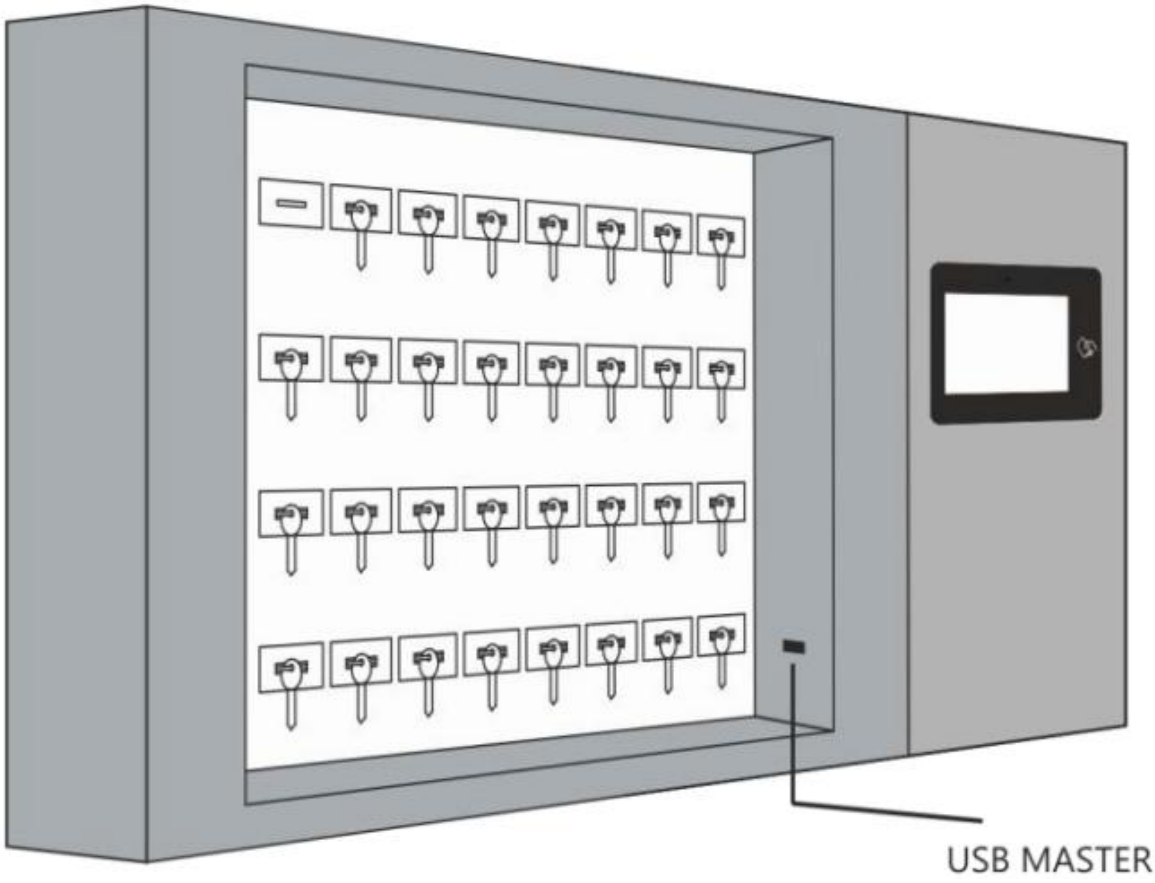

Fig. 2.9. *Socket USB*

3 Primo avvio

Al primo avvio il terminale di controllo MD70 permette di usare la password 9999 per l'utente Master e di selezionare la modalità operativa fra:

- *Any fob position* - le chiavi possono essere restituite inserendole in una qualunque posizione all'interno del deposito chiavi
- *Fixed fob position* - ogni keyfob è assegnato ad uno specifico slot

L'accesso all'app può quindi essere effettuato con 9999# o con 12345*: quest'ultimo è il PIN per chi gestisce il sistema, per esempio per manutenzioni o ragioni di servizio.

Le password di default possono essere personalizzate come descritto più avanti.

Lo schermo del terminale all'avvio si presenta come in Fig. 3.1.

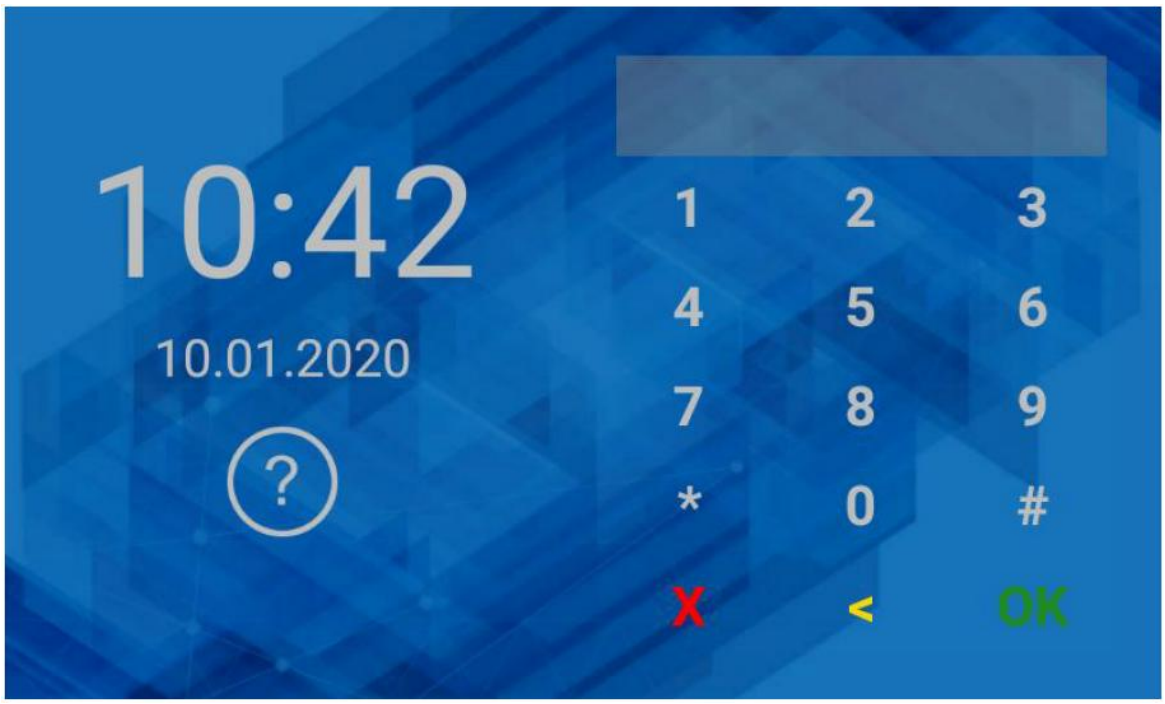

Fig. 3.1. *Schermo terminale all'avvio*

Dopo la password di accesso, compare il menu principale come mostrato in Fig. 3.2.

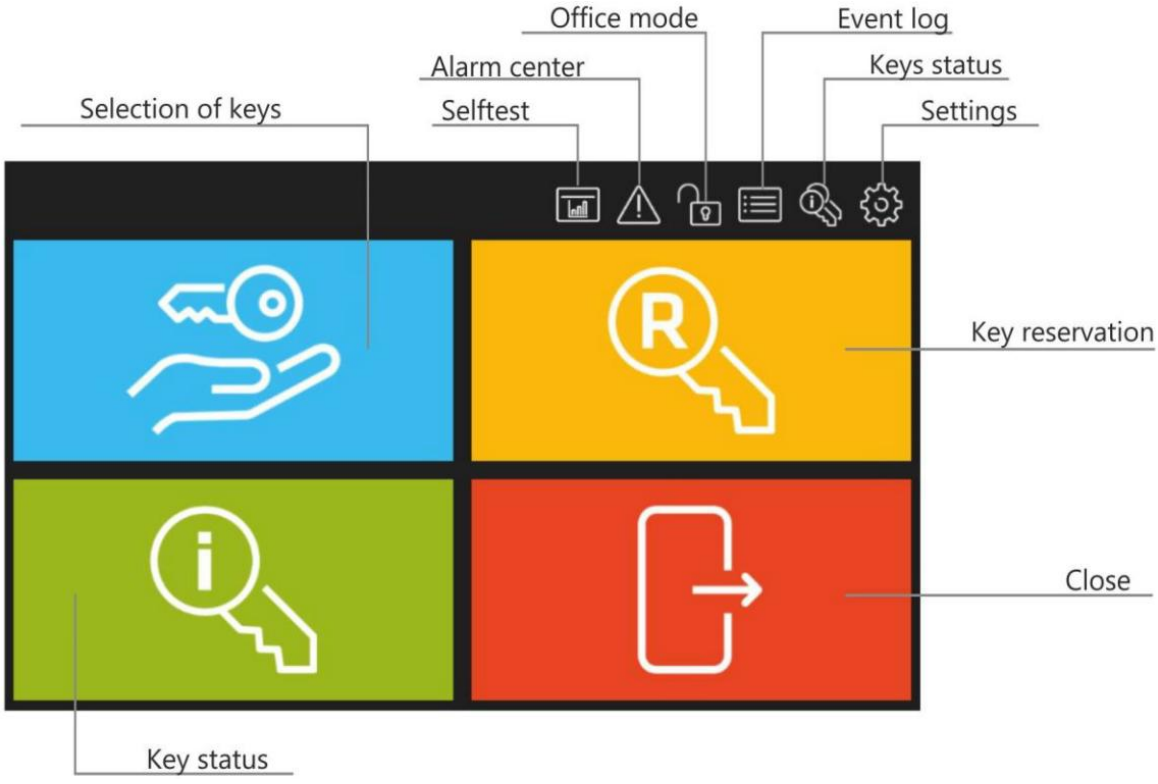

Fig. 3.2. *Menu principale*

Le diverse icone nella barra superiore dello schermo hanno il significato qui sotto riportato.

Indica gli stati di allarme - per esempio porta forzata, tamper, ... - che sono stati registrati dal RKD32 in un lasso di tempo selezionato. Il colore dell'icona indica gli stati seguenti:

- Bianco - nessun allarme
- Arancio - precedenti stati di allarme sono presenti nella memoria
- Rosso - è presente uno stato di allarme non-confermato

Indica la modalità "Office". Se viene selezionata questa modalità, che si avvia al momento di ritorno alla schermata di start (Fig. 3.1), la porta del deposito chiavi è sempre sbloccata, ma i key-fobs che sono programmati come bloccati non sono liberi di essere rimossi dai loro slot. La modalità "Office" può essere soggetta a schedulazione oraria nel menu "*Settings*" - comando "*Office Mode Schedule*".

Avvia il menu Report (vd. Fig. 3.3) nel quale è possibile analizzare gli eventi del sistema - data / ora in cui gli utenti si sono identificati, chiavi prelevate / restituite, ...

Il "*Key report*" mostra gli eventi dove è coinvolta una specifica chiave. Lo "*User Report*" mostra invece i log di uno specifico utente.

È inoltre possibile esportare o eliminare eventi registrati nella memoria del sistema. L'export di eventi (formati XLS e PDF) viene effettuato attraverso la porta USB del Master dove connettere una Pendrive USB.

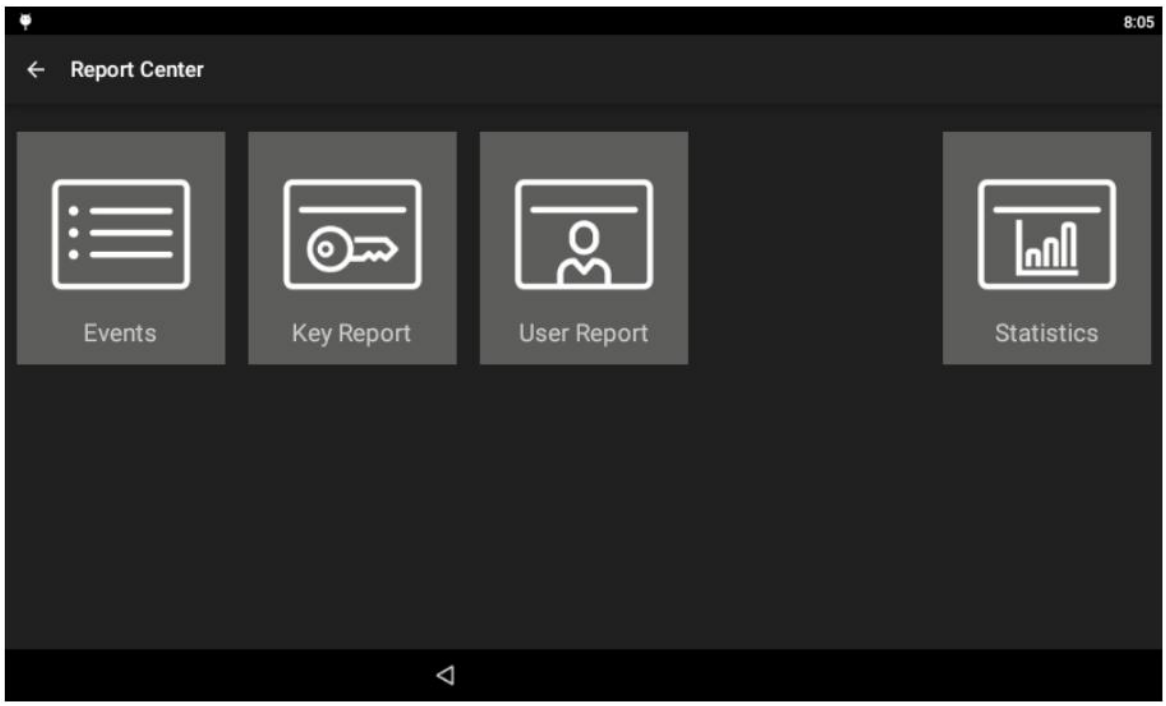

Fig. 3.3. *Menu Report*

Mostra lo stato delle chiavi nel sistema: informa quali chiavi sono state prelevate, chi le ha prelevate e quali chiavi sono prenotate.

Selezionando questa icona si avvia il menu di impostazione - vd. Fig. 3.4.

I sottomenu sono descritti nei successivi pragrafi.

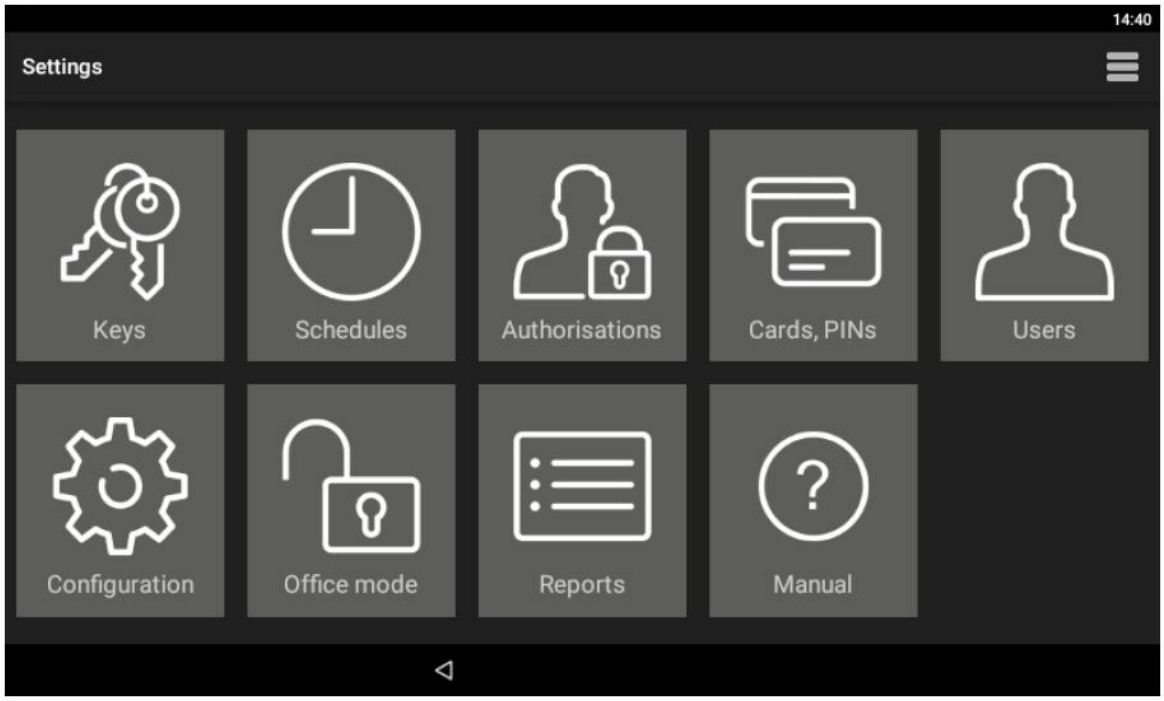

Fig. 3.4. *Menu Settings*

3.1 Keys

Selezionando la prima *tile* del menu *Keys*, viene mostrato l'elenco delle chiavi (cioè dei key-fob) registrate nel sistema. Una nuova chiave può essere registrata con il comando *Add* e quindi leggendo il keyfob sul lettore del terminale di controllo MD70 oppure inserendo il keyfob in uno slot libero del pannello chiavi. Le funzioni di modifica / cancellazione possono essere fatte con un lungo-click di un oggetto nell'elenco.

Assegnando la chiave alla zona interna (*Inner zone*), si può implementare la funzione anti-passback: l'utente può prelevare una chiave da un'altra zona solo quando restituisce tutte le chiavi appartenenti alla *Inner zone*. In sostanza la *Inner zone* è dedicata alle chiavi che devono stare il minor tempo possibile al di fuori del deposito chiavi.

L'opzione "*Required return time*" permette di controllare la restituzione in orario di una chiave. Se si eccede il tempo indicato, viene generato un evento che può essere visualizzato nel centro allarmi.

L'opzione "*Commission get mode*" prevede che per il ritiro di una chiave sia necessaria l'autorizzazione di un altro utente che ha autorizzazione sulla chiave selezionata.

Infine con l'opzione "*Card + PIN mode*" indica che l'utente deve identificarsi sia con il proprio badge sia con il PIN. L'applicazione chiede di leggere la tessera RFID e quindi di confermare con il PIN.

Il gruppo permette di identificare la posizione della chiave nell'elenco degli assets disponibili. Dopo aver selezionato un gruppo specifico, la chiave verrà marcata con il colore definito nella lista.

3.2 Schedules

La seconda *tile* del menu è *Schedules.* Sono presenti due schedulazioni di default "*Always*" e "*Never*". Una nuova schedulazione può essere definita con il comando *Add* e quindi con "*Add range"*. Modifiche e cancellazioni sono possibili da un lungo-click sull'oggetto dell'elenco.

La schedulazione consiste in periodi di tempo che sono specificati in termini di giorni della settimana. La schedulazione può essere usata per limitare le autorizzazioni e gestire l'Office mode.

3.3 Authorisations

Selezionando la terza *tile* del menu, sono mostrate le *Authorisations.* Una nuova *Autorisation* può essere definita con il comando *Add.* Modifiche e cancellazioni sono possibili da un lungo-click sull'oggetto dell'elenco.

Una *Autorisation* può riguardare l'accesso alle chiavi, al menu di impostazioni, ai log di evento, allo stato delle chiavi e può comportare l'abilitazione all'override delle prenotazioni.

Le *Autorisations* sono assegnate agli utenti come descritto nel paragrafo 3.5.

3.4 Cards, PINs

La *tile* del menu "*Cards, PINs"* mostra l'elenco delle tessere e dei PINs del sistema. Le tessere e i PIN sono usati per identificare gli utenti nel terminale MD70. Le funzioni di *Add, Editing, Deleting* sono possibili nell'elenco. Durante l'acquisizione di una tessera, il codice viene letto dal lettore del terminale di controllo MD70.

3.5 Users

Selezionando la *tile* del menu "*Users*" è mostrato l'elenco degli utenti*.* Un utente può essere associato con *Cards*, *Pin* e *Autorisations.* L'opzione *Fob limit* permette di spcificare il numero totale di chiavi che l'utente può prelevare nello stesso istante. Il valore 0 indica nessun limite.

In aggiunta possono essere abilitate le funzioni "*Quick key get mode*" e "*Master exemption*": nel primo caso si abilita lo sblocco automatico delle chiavi autorizzate quando l'utente di identifica sul terminale MD70. Nel secondo caso si assegnano autorizzazioni illimitate per quell'utente.

3.6 Configuration

Selezionando la *tile* del menu "*Configurations*" si possono impostare i parametri specificati nella tabella seguente.

PARAMETRO	SIGNIFICATO
General	
Admin password	È la password di login al terminale MD70, lunga da 4 a 10 cifre. Di default la password è 12345. La password viene terminata col carattere *.
Logout when door closed	Il parametro abilita il logout automatico dell'utente e riporta lo schermo alla pagina iniziale quando la porta del deposito chiavi viene chiusa. Valori: ON, OFF. Default: ON.
Automatic logout time (sec)	Il parametro definisce il tempo dopo il quale l'utente è automaticamente in logout e lo schermo ritorna alla pagina iniziale se non viene effettuata alcuna azione sui menu del terminale. Range: 0-99 s. Default: 60 s.
Automatic logout	Il parametro permette il logout automatico dell'utente e il ripristino dello schermo del terminale alla pagina iniziale quando termina il tempo *Automatic logout time*. Valori: ON, OFF. Default: ON.
Alarm signaling time (min)	Il parametro definisce il tempo per la segnalazione dell'allarme tamper sull'output LCK4. Range: 0-99. Default: 3.
Door open too long prealert time (s)	Il parametro definisce il tempo della segnalazione acustica al terminale MD70 quando la porta è aperta e l'utente è in logout. Range: 0-99. Default: 60.
Fire alarm support	Il paramero permette il rilascio in emergenza della porta e di tutti i blocchi chiave fintantoché l'ingresso digitale DR3 è triggerato da un sistema esterno, es. Sistema anti-incendio. Valori: ON, OFF. Default: OFF.
Office mode	Selezionando questa opzione, la porta del deposito chiavi è aperta ma le chiavi rimangono bloccate nei propri slot. Default: OFF.
Selective cabinet's opening	Selezionando questa opzione, verranno aperte le porte dei soli pannelli dove sono presenti le chiavi disponibili, dopo che l'utente si sia identificato.
Fast relogin	Dopo aver attivato questa opzione, è possibile eseguire una nuova identificazione utente senza eseguire il logout dell'utente precedente: ciò avviene semplicemente leggendo la tessera dell'utente successivo.
Events with photos	Opzione che permette di effettuare una foto all'utente che si identifica sul terminale MD70.
Keys	
Quick key return mode	È la modalità nella quale per la restituzione della chiave non è richiesta l'identificazione dell'utente mediante badge o PIN: l'utente apre la porta e restituisce la chiave in uno slot libero. Valori: ON, OFF. Default: ON.
Show absent key on list	Il parametro permette di mostrare le chiavi prelevate sia nella finestra di selezione chiavi che nella finestra di stato chiavi. Valori: ON, OFF. Default: ON.
Fast get: show absent key info	Il parametro permette di mostrare le chiavi al momento non disponibili per il ritiro: quando l'utente si identifica al terminale viene mostrato un messaggio sullo schermo. Valori: ON, OFF. Default: OFF.

Function: identify key	Dopo aver selezionato questa opzione, è possibile identificare la chiave. Per poterla identificare, leggere il keyfob sul lettore del terminale MD70 dopo essersi identificati con le proprie credenziali.
Shortcut to getting key	Display automatico dell'elenco chiavi dopo il login. L'opzione è disponibile solo se è disattivata la prenotazione chiavi e nel modo di posizionamento chiavi non fisso. L'utente inoltre non deve aver accesso alle pagine di impostazione. Default: OFF.
Shortcut: logout after get single key	Il parametro attiva il logout automatico dopo il prelievo di una singola chiave. Il parametro funziona se l'opzione "*Shortcut to getting key*" è attiva. Defualt: OFF.
Email notification	Abilitando questo parametro si inviano notifiche email circa gli eventi di allarme e quando la restituzione chiave avviene con ritardo.
Comments	
Reporting a comment about the equipment status	Attivando questa opzione, un box di dialogo verrà mostrato durante il prelievo e la restituzione della chiave: è possibile aggiungere un commento sullo stato della chiave o altre richieste dell'amministratore.
Comments on demand	Questa opzione abilita la possibilità di immettere un commento in qualunque momento. L'opzione rimpiazza l'icona di prenotazione chiave.
Predefined comment content (1)	Immettere il testo che apparirà come opzione di controllo quando sarà riportato un commento.
Predefined comment content (2)	Immettere il testo che apparirà come opzione di controllo quando sarà riportato un commento.
Predefined comment content (3)	Immettere il testo che apparirà come opzione mentre si scrive il commento. Il contenuto predefinito può essere completato dall'utente, per esempio dopo aver inserito il testo "Kilometraggio Km:" l'utente può immettere il valore del contachilometri al momento della restituzione della chiave. NOTA: se nessuno dei tre testi è definito, rimane valida la sola opzione per immettere il proprio commento.
Reservation	
Disable reservations	Il parametro blocca la possibilità di prenotare una chiave. Default: OFF.
Block reserved key	Il parametro permette di bloccare una chiave che è stata prenotata. Valori: ON, OFF. Default: OFF.
Maximum reservation time (h)	Il parametro definisce il periodo massimo di prenotazione di una chiave espresso in ore. Range: 0-99. Default: 30.
Display	
Custom wallpaper	Permette di personalizzare lo sfondo dello schermo del terminale MD70. Il wallpaper è indicato dal comando "Select wallpaper" del menu ☰ posto in alto a destra. Valori: ON, OFF. Default: OFF.
Font color	Il parametro permette di specificare il colore del font usato nello schermo di avvio del terminale MD70. Valori: Light, Dark, Orange. Default: Light.
Voice prompts	Opzione che abilita l'emissione di messaggi vocali. Default: OFF.

WWW settings	
Web access enable	Il parametro permette la configurazione e la gestione del pannello RKD32 via web browser.
Port	Il parametro definisce la porta di comunicazione per l'accesso via web browser. Per ragioni di sicurezza, il valore della porta non può essere inferiore a 1024. Default: 8888.
Login	Il parametro definisce il login per l'accesso via web browser.
Password	Il parametro definisce la password di accesso via web browser.
Email account	
Address	Account email usato per l'invio di messaggi e report da parte del RKD32.
Login	Login dell'account email per l'invio da parte del RKD32.
Password	Password dell'account email per l'invio di email da parte del RKD32.
SMTP port	Porta email. Default: 587.
Host	Indirizzo host email.
SSL	Parametro per abilitare la criptazione SSL per l'invio di email. Valori: ON, OFF. Default: OFF.
Address 1	Indirizzo email del destinatario.
Address 2	Indirizzo email addizionale del destinatario.

Il menu che compare in alto a destra del menu di Configurazione (icona ☰) permette i comandi indicati nella tabella qui sotto riportata.

COMANDO	SIGNIFICATO
Select walpaper	Comando per selezionare uno sfondo dello schermo personalizzato nel terminale MD70. Il formato deve essere JPG e le dimensioni devono essere 800x480 px. Il parametro "*Custom walpaper*" deve essere abilitato.
Detect devices	Il comando avvia una ricerca dei dispositivi nel sistema RKD32. Dopo aver aggiunto un modulo di espansione RKD32EXT, eseguire questo comando per rilevare i nuovi dispositivi.
Office mode schedule	Il comando assegna una schedulazione all'Office mode. La schedulazione può essere definita nelle Schedules.
Key slot settings	Il comando abilita la regolazione del livello di luce degli slot delle chiavi.
Check for update	Il comando controlla e scarica via rete gli aggiornamenti del software. È necessario che RKD32 sia connesso alla rete e a Internet.
Install update	Qualora aggiornamenti fossero stati scaricati, il comando permette di installarli.
Import users from PRMaster	Il comando abilita l'importazione di utenti dal software PR Master di un sistema RACS4.
Configuration export	Il comando permette di esportare le impostazioni di configurazione per effettuare un backup o utilizzare le stesse impostazioni su un altro RKD32.
Configuration import	Il comando ripristina la configurazione da un backup.

Factory reset	Il comando ripristina le impostazioni di fabbrica del dispositivo.

3.7 Office mode

Selezionando la *tile* del menu "*Office mode*", viene avviata l'opzione come descritto precedentemente all'inizio del capitolo 3.

3.8 Reports

Selezionando la *tile* del menu "*Reports*", viene avviata l'opzione come descritto precedentemente all'inizio del capitolo 3.
In particolare "*Key report*" mostra gli eventi relativi ad una particolare chiave. I log possono essere eliminati, esportati su una memoria esterna o inviati via email.

3.9 Manual

L'utima *tile* del menu è "*Manual*": viene mostrato il Manuale di uso dell'app nello schermo del terminale MD70.

3.10 Menu

Il menu della finestra mostrata in Fig. 3.4 include comandi addizionali differenti da quelli descritti nella tabella della pagina precedente. Questi comandi sono descritti nella tabella seguente.

COMANDO	SIGNIFICATO
Show launcher	Il comando abilita l'uscita dall'App RKD32 e l'avvio dell'ambiente Android. La password di default è admin.
System settings	Il comando abilita la configurazione del s.o. Android.
MD70 settings	Il comando abilita la configurazione di altri parametri del terminale MD70.
Files	Il comando avvia l'app che permette l'esplorazione dei file del terminale MD70.
About	Il comando mostra il registro delle modifiche.
License	Il comando mostra la licenza del software Roger.
License file	Il comando mostra le informazioni di licenza caricate nel RKD32 in relazione al modo di lavoro in rete via browser.
Export database	Il comando abilita l'esportazione delle impostazioni di RKD32 su pendrive.
Import database	Il comando abilita l'importazione delle impostazioni di RKD32 da un file presente su pendrive.
Remote support	Il comando abilita la connessione remota di un terminale MD70 per analisi tecniche / diagnostiche da parte di tecnici del produttore.

4 Configurazione in standalone e in rete

In questo capitolo vengono descritte le azioni da intraprendere per la configurazione in modo stand-alone.

4.1 Chiavi

- Abbinare meccanicamente le chiavi ai keyfob
- Effettuare il login al terminale (default PIN: 9999#) e selezionare l'icona "*Settings*" raffigurata come un ingranaggio e quindi l'icona "*Keys*"
- Nella successiva finestra selezionare "*Add*"
- Nella successiva finestra fornire un nome alla chiave, per esempio "Veicolo 1" e poi leggere il keyfob con il lettore del terminale MD70 o inserire il keyfob in uno slot libero
- Impostare le opzioni per quella chiave come necessario
- Effettuare le medesime operazioni per tutte le altre chiavi

4.2 Schedulazioni (Opzionale)

- Effettuare il login al terminale (default PIN: 9999#) e selezionare l'icona "*Settings*" raffigurata come un ingranaggio e quindi l'icona "*Schedules*"
- Nella successiva finestra selezionare "*Add*"
- Nella successiva finestra fornire un nome alla schedulazione e clickare su "*Add range*"
- Specificare il periodo per i giorni della settimana. La schedulazione può essere applicata per le autorizzazioni e per l'Office mode.

4.3 Autorizzazioni

- Effettuare il login al terminale (default PIN: 9999#) e selezionare l'icona "*Settings*" raffigurata come un ingranaggio e quindi l'icona "*Authorisations*"
- Nella successiva finestra selezionare "*Add*"
- Nella successiva finestra fornire un nome all'autorizzazione e clickare su "*Location*" per indicare le chiavi che potranno essere ritirate da parte degli utenti dotati di quell'autorizzazione
- In opzione, clickare su "*Schedule*" e assegnare una schedulazione precedentemente creata all'autorizzazione.
- In aggiunta, si può selezionare se l'autorizzazione fornisce accesso al menu di impostazioni, log eventi e stato delle chiavi e inoltre se è abilitata alla sovrascrittura di prenotazioni chiave.

4.4 Card, PIN

- Effettuare il login al terminale (default PIN: 9999#) e selezionare l'icona "*Settings*" raffigurata come un ingranaggio e quindi l'icona "*Cards, PINs*"
- Nella successiva finestra selezionare "*Add Card*" oppure "*Add PIN*". Nel primo caso, l'ID della tessera può essere letto dal lettore del terminale MD70 dopo aver clickato "*Card code*".

4.5 Utenti

- Effettuare il login al terminale (default PIN: 9999#) e selezionare l'icona "*Settings*" raffigurata come un ingranaggio e quindi l'icona "*Users*"
- Nella successiva finestra selezionare "*Add*"
- Nella successiva finestra fornire un nome all'utente. Clickare su "*Cards, PINs*" per assegnare la credenziale prcedentemente memorizzata nel terminale MD70. Clickare su "*Authorisations*" per assegnare una autorizzazione precedentemente creata che specifica quali chiavi possono essere prelevate da quell'utente in una particolare schedulazione temporale.
- In opzione si può abilitare il parametro "*Quick get key mode*" o il parametro "*Master exemption*". L'ultima opzione è normalmente abilitata per amministratori o operatori di sistema. Il parametro "*Fob limit*" diverso da zero limita il numero di chiavi che l'utente può prelevare.

4.6 Import Utenti da PRMASTER - RACS 4

Gli utenti definiti in un sistema RACS4 nel database del software PR MASTER, possono essere importati con le medesime credenziali nell'app del RKD32.

- Avviare PR Master, selezionate "Utenti" e quindi "Export" così da generare un file contenente gli utenti con i codici delle tessere RFID e i PIN a loro assegnati. Il file esportato è PRM.CSV.
- Se fosse necessario preservare caratteri non-latini, aprire PRM.CSV con il programma di Windows "Notepad" e salvare il file con codifica UTF-8.
- Copiare il file PRM.CSV su una Pendrive.
- Collegare la Pendrive alla porta USB Master (vd. Fig. 2.9).
- Eseguire il login (default PIN: 9999#), selezionare l'icona che raffigura l'ingranaggio e quindi "*Configuration*".
- Nella successiva finestra selezionare ☰ e infine la voce "*Import users from PR Master*".

4.7 Prenotazione di una chiave

Una chiave può essere prenotata selezionando la tile ® del menu principale (vd. Fig. 3.2) e quindi usando il comando "*Add*". Nella successiva finestra deve essere specificato un intervallo orario e quindi selezionata l'opzione "*Block key during reservation*".

Se l'opzione globale "*Block reserved key*" è abilitata (vd. Paragrafo 3.6 Configuration) allora tutte le chiavi sono bloccate per default durante il periodo di prenotazione. La chiave che è prenotata senza essere bloccata può essere prelevata durante il periodo di

prenotazione da un altro utente che è autorizzato per quella chiave: in tal caso, al momento del prelievo è solo mostrato un avviso della prenotazione in atto.

L'utente a cui è assegnata con l'autorizzazione anche l'opzione "*Key reservation override authorisation*" può prelevare le chiavi prenotate senza alcun limite incluse le chiavi prenotate con blocco di prenotazione.

4.8 Configurazione via web browser

RKD32 può essere configurato e gestito via rete con software fornito in licenza.

In questo scenario, è necessario definire i parametri nella sezione "*WWW settngs*" - vd. Paragrafo 3.6 Configuration.

La comunicazione con il terminale MD70 può essere via rete cablata (porta Ethernet) o WLAN. L'indirizzo IP del pannello è configurato dopo essere usciti dall'applicativo RAACA con il comando "*Show launcher*" (vd. Paragrafo 3.10 Menu).

Prima di stabilire una connessione con il pannello RKD32 è necessario immettere l'indirizzo IP e la porta di comunicazione (per default: 8888). Per l'accsso alla porta, potrebbe essere necessario agire sul firewall di rete e/o sul software antivirus.

NOTA.

La configurazione via web browser richiede l'acquisto della licenza del software. Per verificare se la licenza è attiva per il vostro RKD32, selezionare "*License file*" nel menu descritto al paragrafo 3.10.

La pagina di login del software è mostrata in Fig. 4.1.

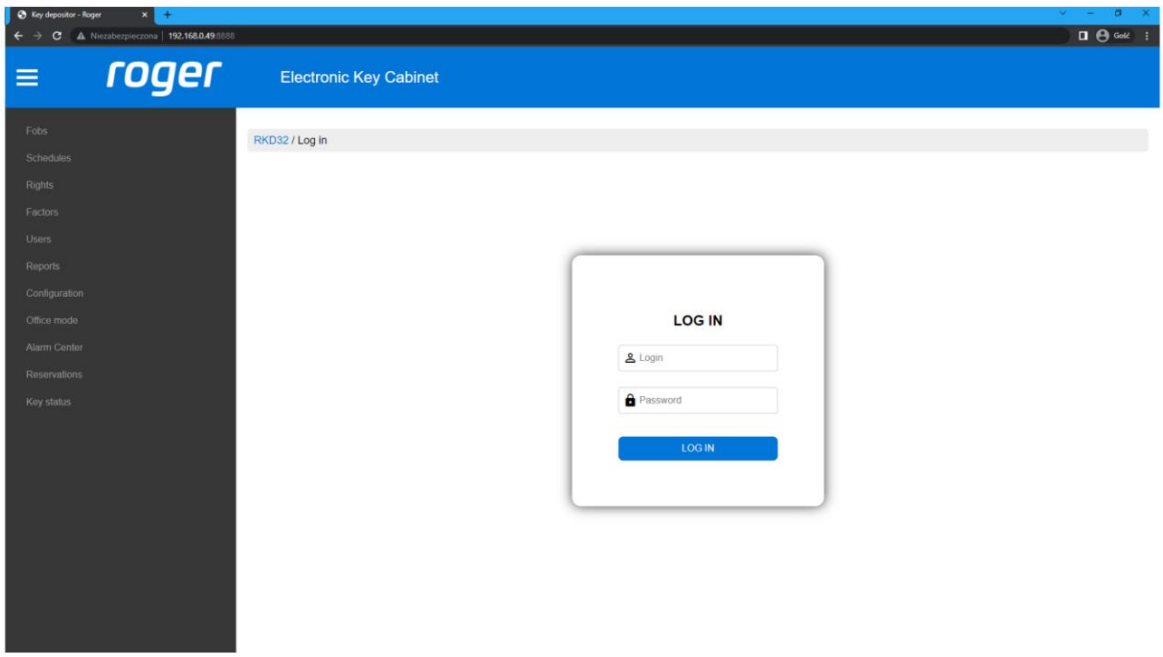

Fig. 4.1. *Login software per la configurazione via web browser*

5 Gestione e attività generali

In questo capitolo sono descritte le principali funzioni e una sezione di "troubleshooting".

5.1 Modifica PIN Admin

- Eseguire il login (default PIN: 9999# oppure 12345*), selezionare e poi "*Configuration*".
- Clickare "*Admin password*" e rimpiazzare la password di default 12345 con quella a vostra scelta.

5.2 Modifica PIN Master

- Eseguire il login (default PIN: 9999# oppure 12345*), selezionare e poi "*Cards, PINs*".
- Selezionare "*Add PIN*" così da definire una nuova credenziale e poi ritornare alla finestra di impostazioni.
- Selezionare "*Users*".
- Effettuare un click lungo su *USER_ADMIN* e quindi selezionare "*Edit*".
- Clickare "*Cards, PINs*", deselezionare il *PIN_ADMIN* di default (9999) e selezionare il PIN a vostra scelta.

5.3 Tessere programmabili

Per default, il lettore del terminale MD70 legge il numero seriale delle tessere MIFARE (CSN), ma è possibile programmare delle tessere con un proprio codice (PCN) in specifici settori criptati della memoria delle tessere. L'uso del codice PCN previene la clonazione delle tessere e quindi il loro possibile uso fraudolento. Per configurare come il terminale leggerà il codice delle tessere, seguire la procedura qui sotto riportata:

- Eseguire il login (default PIN: 9999#) e selezionare .
- Nella successiva finestra selezionare e quindi la voce "*MD70 settings*".

NOTA.

Se il metodo di lettura dei codici tessera non è quello di default (CSN), allora il lettore integrato nel terminale non potrà essere usato per l'acquisizione dei codici e per la funzione "*Quick fob return mode*".

Per la programmazione dei codici PCN utilizzare l'accessorio RUD-3-DES.

Questo paragrafo ha significato solo se vengono utilizzate tessere Mifare con settori di memoria codificabili secondo le proprie esigenze, per esempio badge Mifare Classic 1k.

5.4 Backup impostazioni

Le impostazioni del pannello RKD32 (incluso l'elenco degli utenti e le loro credenziali) può essere esportato su file con lo scopo di ottenere una copia di backup. **L'esportazione delle impostazioni è fortemente consigliata**, anche nel caso di utilizzo del software in licenza via browser: alcune impostazioni vengono memorizzate esclusivamente nel terminale MD70.

5.5 DataBase Esport

- Connettere una pendrive alla porta USB Master (vd. Fig 2.9).
- Eseguire il login (default PIN: 9999# oppure 12345*), selezionare ⚙ e poi ☰.
- Selezionare il comando "*Export DataBase*".

5.6 DataBase Import

- Rinominare il database precedentemente esportato nel file RKDdb.db e copiarlo su una pendrive.
- Connettere una pendrive alla porta USB Master (vd. Fig 2.9).
- Eseguire il login (default PIN: 9999# oppure 12345*), selezionare ⚙ e poi ☰.
- Selezionare il comando "*Import DataBase*".

5.7 Rilascio chiavi in emergenza

La porta dell'RKD32 e le chiavi possono essere sbloccate in mancanza di alimentazione. In questo caso connettere un powerbank (con corrente di output min 2A) alla porta USB posta sotto al flap di emergenza e rilasciare la porta e le chiavi premendo i pulsanti DOOR e ROW-1/2/3/4. La procedura deve essere ripetuta per ciascun RKD32 individualmente, nel caso fossero installate delle espansioni.

5.8 Ripristino condizioni di fabbrica

Per riottenere le impostazioni di fabbrica, seguire la procedura seguente:

- Eseguire il login (default PIN: 9999# oppure 12345*), selezionare ⚙ e poi "*Configuration*".
- Nella successiva finestra selezionare ☰ e quindi la voce "*Factory reset*".

5.9 Attivazione licenza

Nel caso sia richiesta la gestione del sistema RKD32 via web browser, è necessario attivare la licenza nel sistema. Per verificare lo stato della vostra licenza, selezionare il comando "*License file*" come descritto nel paragrafo 3.10.

Per caricare la licenza acquistata, copiare il file di licenza in una memoria USB o nella memoria interna del terminale. Quindi eseguire l'app "*RKD receiver*" e importare la licenza.

5.10 Troubleshooting

PROBLEMA	SOLUZIONE
La chiave è inserita nello slot ma non è presente nell'elenco delle chiavi	▪ Verificare "*Authorisations*" e "*Schedules*" dell'utente ▪ Verificare se l'utente con "*Master exemption*" può individuare la chiave nell'elenco.
La chiave non può essere prelevata per assenza alimentazione	▪ Seguire le istruzioni riportate nel paragrafo 5.7.
Il key-fob non può essere letto dal terminale MD70	▪ La portata di lettura del key-fob è limitata a causa delle sue dimensioni. Seguire le indicazioni riportate nel paragrafo 2.4.
La pagina di avvio non è mostrata nel terminale MD70	▪ Riavviare il terminale MD70 spegnendolo con il pulsante di riavvio (vd. Fig. 5.1) ▪ Riavviare l'app RAACA manualmente
Il terminale MD70 non reagisce al tocco sullo schermo	▪ Verificare l'alimentazione ▪ Riavviare il terminale MD70 spegnendolo con il pulsante di riavvio (vd. Fig. 5.1)

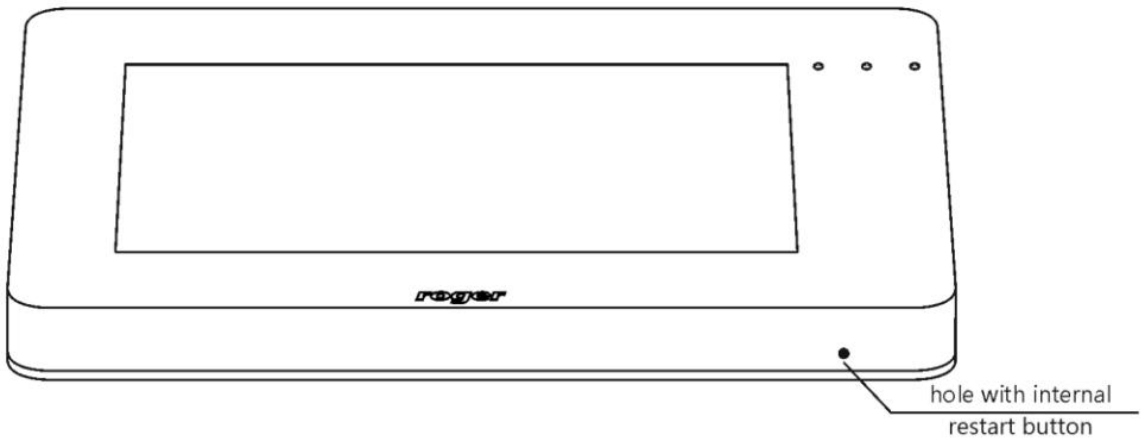

Fig. 4.1. *Pulsante di riavvio del terminale Android MD70*