



Accesso a B&B

Guida rapida

Installazione e Utilizzo

Versione 2.1, Maggio 2024

© 2007 – 2024 DOINGPRO Srl, all rights reserved



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



DOINGPRO SRL si riserva il diritto di apportare qualunque cambiamento al presente manuale in qualunque parte senza preavviso scritto.

DOINGPRO SRL ha dedicato il massimo sforzo per assicurare che il presente documento sia preciso nelle informazioni fornite; tuttavia, DOINGPRO SRL non si assume alcuna responsabilità per eventuali errori ed omissioni, con ciò includendo qualsiasi danno risultante dall'uso delle informazioni contenute nel presente manuale.

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

Tel.: +39 329 2288344

email: info@doingsecurity.it



Indice

Indice	3
1 Introduzione	4
1.1 Utilizzo del prodotto	5
1.2 Specifiche tecniche BS200K	6
1.3 Specifiche tecniche FL200KCS	6
1.4 Specifiche tecniche Gateway G2	7
1.5 Avvertenze	7
1.6 Terminologia	7
2 Installazione	9
2.1 Tastiera BS200K	9
2.2 Gateway WiFi	11
2.3 Maniglia FL200KCS	12
3 Programmazione del sistema	13
3.1 Download APP	13
3.2 Account	14
3.3 Setup	15
3.4 Aggiunta Gateway, Tastiere e Serrature	15
3.5 Definizione PIN e Tessere RFID	18
3.5.1 Generare un codice PIN	20
3.5.2 Associare una tessera RFID	21
3.6 Log Accessi	23
3.7 Funzioni Avanzate	24
3.8 Opzioni	25



1 Introduzione

Il presente documento illustra come installare e utilizzare il sistema dedicato ai B&B per il controllo di accesso wireless mediante tastiere Bluetooth gestibili - attraverso un Gateway WiFi - con codici PIN, tessere RFID e comandi via smartphone.

Il Manuale descrive le diverse operazioni di posa degli apparati, di programmazione e gestione degli accessi e comprende le istruzioni per l'uso e la configurazione del prodotto.

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.

Tutte le informazioni, comprese, tra le altre, formulazioni, immagini e grafica sono di proprietà di DOINGPRO SRL. Questo manuale non può essere riprodotto, modificato in alcun modo o distribuito anche in parte con qualsiasi mezzo senza la preventiva autorizzazione scritta di DOINGPRO SRL.

Salvo disposizioni contrarie, DOINGPRO SRL 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: DOINGPRO SRL 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 DOINGPRO SRL, 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 DOINGPRO SRL 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: DOINGPRO SRL 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 DOINGPRO SRL 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: DOINGPRO SRL 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 tastiera BS200K - compresi gli accessori di montaggio
- Per alimentare il Gateway, usare l'alimentatore da smartphone fornito con uscita USB per la ricarica a 5V @ 500 mA
- Assicurarsi di conoscere la password di accesso del proprio WiFi
- Scaricare l'APP "TTLOCK" dallo Store Apple o da Google Play
- 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.

Tipicamente l'architettura di un sistema è illustrata in Fig. 1.1.

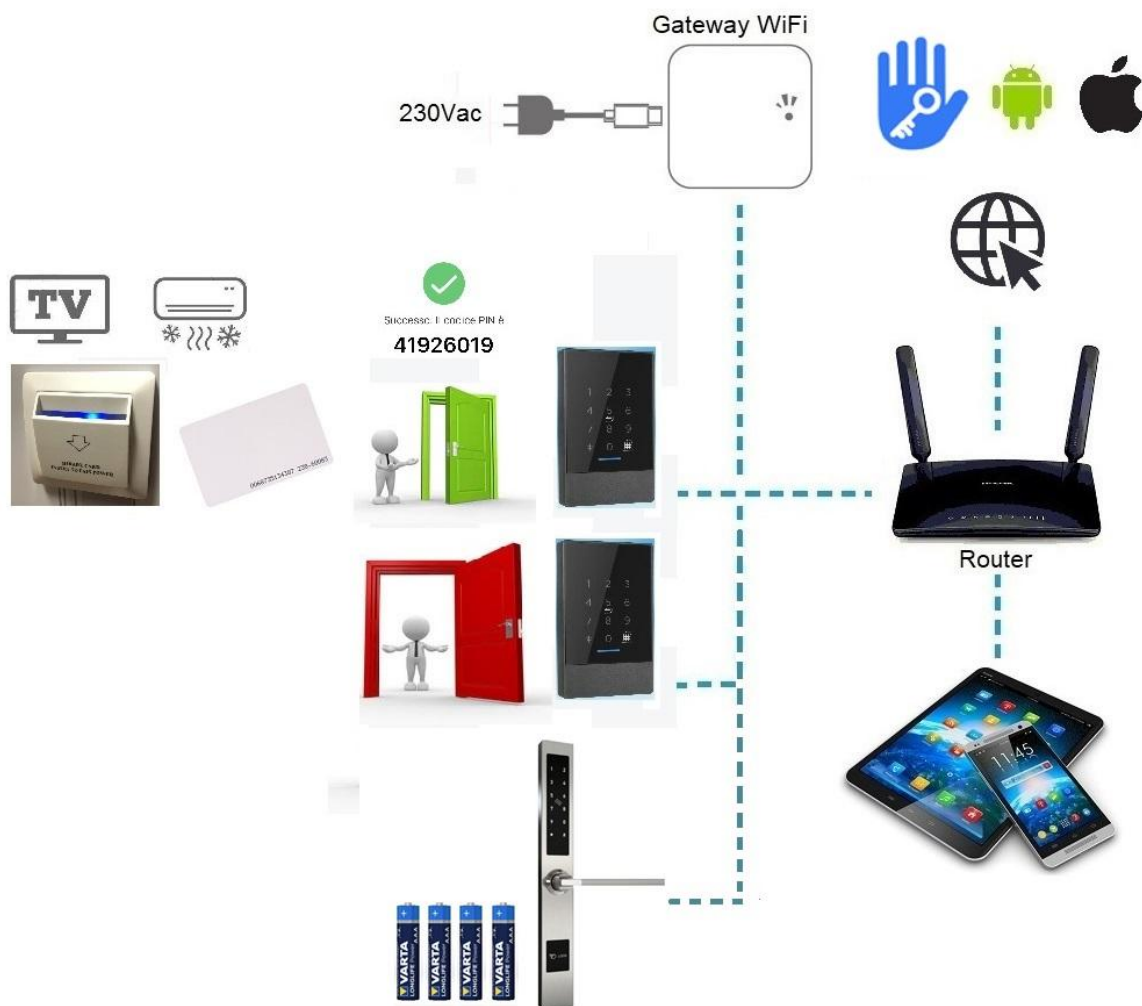


Fig. 1.1. *Architettura sistema*



1.2 Specifiche tecniche BS200K

Le principali caratteristiche e prestazioni della tastiera BS200K sono elencate nella tabella sottostante.

□ Prestazione	Descrizione
CPU e memoria	CPU a 32 bit, memoria per 20.000 codici RFID
Materiale	Alluminio con frontale in vetro temperato (tastiera "touch")
Credenziali per l'apertura	Bluetooth, codice PIN o Tag Mifare® classic ISO/IEC 14443-A
Comunicazione	Bluetooth verso il Gateway
Sistemi supportati	Android 4.3 o superiore / iOS 7.0 o superiore
Montaggio	A filo muro o porta
Alimentazione e consumo	12 Vcc @ 1A max (in stand-by 5 mA circa)
Input / Output	Ingresso stato porta e ingresso pulsante di uscita / Uscita relè NA-COM-NC e allarme / Funzione campanello
Segnalazioni LED	Verde e rosso
Tempo di apertura	1,5 s
Uso	Stand-alone oppure in rete con Gateway wireless e APP "TTLOCK"
Grado di protezione	IP65 per uso interno / esterno
Peso e dimensioni	0,29 kg - 125 (A) x 79 (L) x 15,5 (P) mm.
Condizioni operative	Temperatura: -10°C ~ +55°C, U.R. 30% ~ 95%

1.3 Specifiche tecniche FL200KCS

Le principali caratteristiche e prestazioni della tastiera FL200KCS sono elencate nella tabella sottostante.

□ Prestazione	Descrizione
CPU e memoria	CPU a 32 bit, memoria per 200 codici PIN e 200 codici RFID
Materiale	Acciaio INOX AISI 304 con inserti in vetro temperato (tastiera "touch")
Credenziali per l'apertura	Bluetooth, codice PIN o Tag Mifare® classic ISO/IEC 14443-A
Comunicazione	Bluetooth verso il Gateway
Sistemi supportati	Android 4.3 o superiore / iOS 7.0 o superiore
Montaggio	Su porta con serratura EURO (es. 7085). Passo fra maniglia e cilindro 85 mm.
Alimentazione e consumo	4 batterie alcaline AAA, tip. 18 mesi di vita utile delle batterie
Segnalazioni utente	LED e buzzer. Avviso batteria bassa
Tempo di apertura	1,5 s
Uso	Stand-alone oppure in rete con Gateway wireless e APP "TTLOCK"
Grado di protezione	In interno
Peso e dimensioni	1,2 kg - 310 (A) x 40 (L) x 20 (P) mm.
Condizioni operative	Temperatura: -10°C ~ +55°C, U.R. 30% ~ 95%



1.4 Specifiche tecniche Gateway G2

Le principali caratteristiche di Gateway G2 sono elencate nella tabella sottostante.

☐ Prestazione	Descrizione
Comunicazione	WiFi 2.4G, 802.11 b/g/n. Disponibile anche in versione PoE (cod. G3)
Alimentazione	Mediante interfaccia USB tipo-C, cavo USB A-C in dotazione, 5V @ 500 mA
Segnalazioni LED	Alternato ROSSO-BLU: in fase di ricerca rete WiFi (pairing mode mediante APP) Blu lampeggiante: in modo operativo standard Rosso fisso: Assenza di rete o guasto
Conformità	CE e FCC Part 15
Segnalazioni LED	Blu e rosso
Precauzioni di uso	Uso in interno a distanza da altre antenne o trasmettitori per eliminare interferenze
Grado di protezione	IP41 per uso interno
Peso e dimensioni	0,15 kg - 70 (A) x 70 (L) x 26 (P) mm
Condizioni operative	Temperatura: 5°C ~ +45°C, U.R. 30% ~ 95%

1.5 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)
- Direttiva 2014/30/EU (EMC)
- Direttiva 2014/53/EU (RED)
- Direttiva 2011/65/EU (RoHS)



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.

1.6 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. Ciascun standard 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 pacchetti del protocollo **UDP/TCP/IP** nelle reti di computer. È usato per effettuare telefonate via Internet, Intranet o altre tipologie di connessioni dati
- **TCP/IP** contiene un set di protocolli per la comunicazione nelle reti di computer ed 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 sincronizzazione 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
- **Wiegand** è un protocollo standard utilizzato nei sistemi di controllo degli accessi, comunemente utilizzato per connettere mediante doppino twistato un lettore di tessere ad un controllore di accesso con una comunicazione mono-direzionale per una distanza di massimo qualche decina di metri (tipicamente 100 metri).
- **OSDP** (Open Supervised Device Protocol - IEC60839-11-5) è uno standard sviluppato dalla Security Industry Association (SIA) per offrire comunicazioni di controllo degli accessi più sicure fra i lettori di identificazione e i controllori di accesso. Utilizza un bus RS485 (doppino twistato) e comporta una comunicazione dati criptata



2 Installazione

2.1 Tastiera BS200K

La tastiera di accesso è mostrata in Fig. 2.1.



Fig. 2.1. BS200K

Il kit di accessori contenuti nella confezione sono mostrati in Fig. 2.2. Gli accessori di installazione sono necessari e sufficienti per la posa della tastiera.

Placca a muro



Cavo



Viti e tasselli



Chiave Allen



Fig. 2.2. Accessori BS200K



La posa della tastiera è mostrata nella Fig. 2.3.

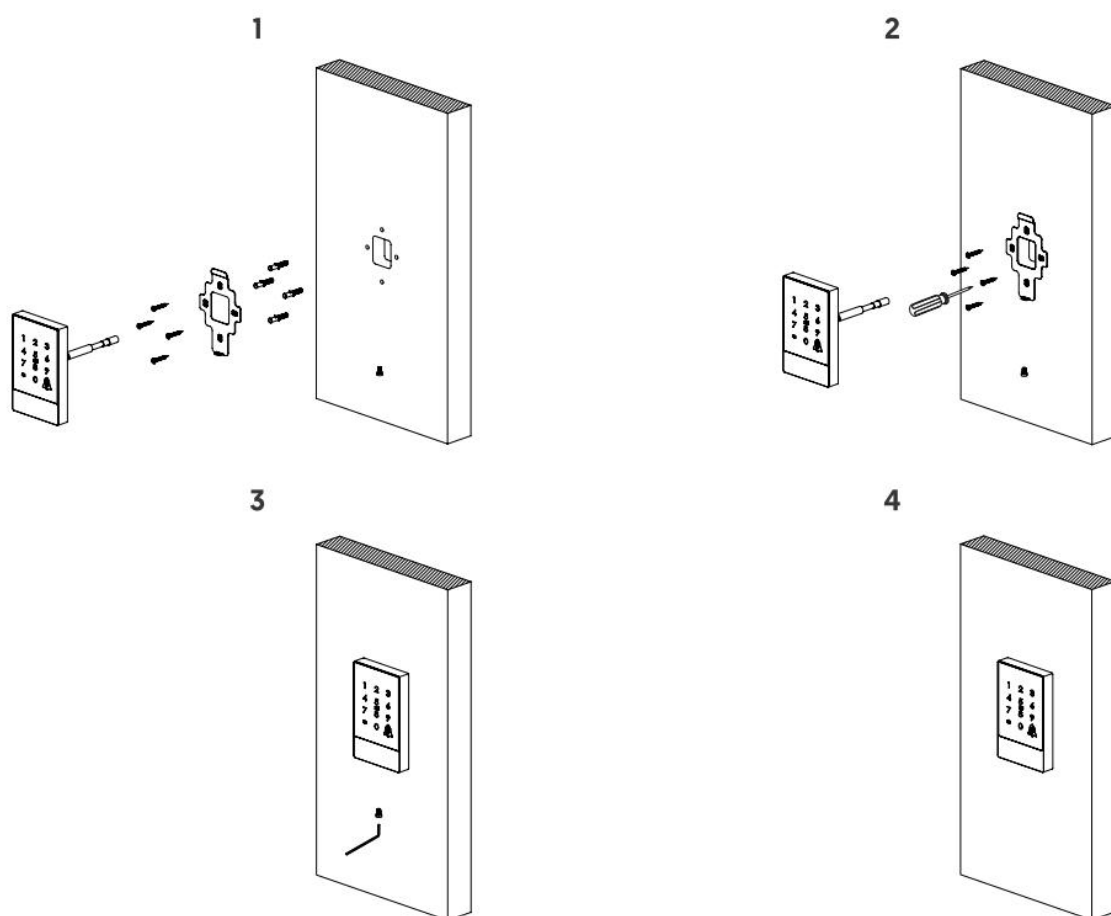


Fig. 2.3. Posa di BS200K

Per i collegamenti elettrici far riferimento alla Fig. 2.4 e alla seguente tabella con i codici colore dei diversi poli:

COLORE	SIGNIFICATO
Rosso	12Vcc
Nero	GND
Arancio	NC relè di apertura
Giallo	COM relè di apertura
Verde	NA relè di apertura
Blu	Ingresso per pulsante uscita
Viola	Ingresso stato porta
Bianco	Allarme
Grigio	Campanello
Marrone	Campanello

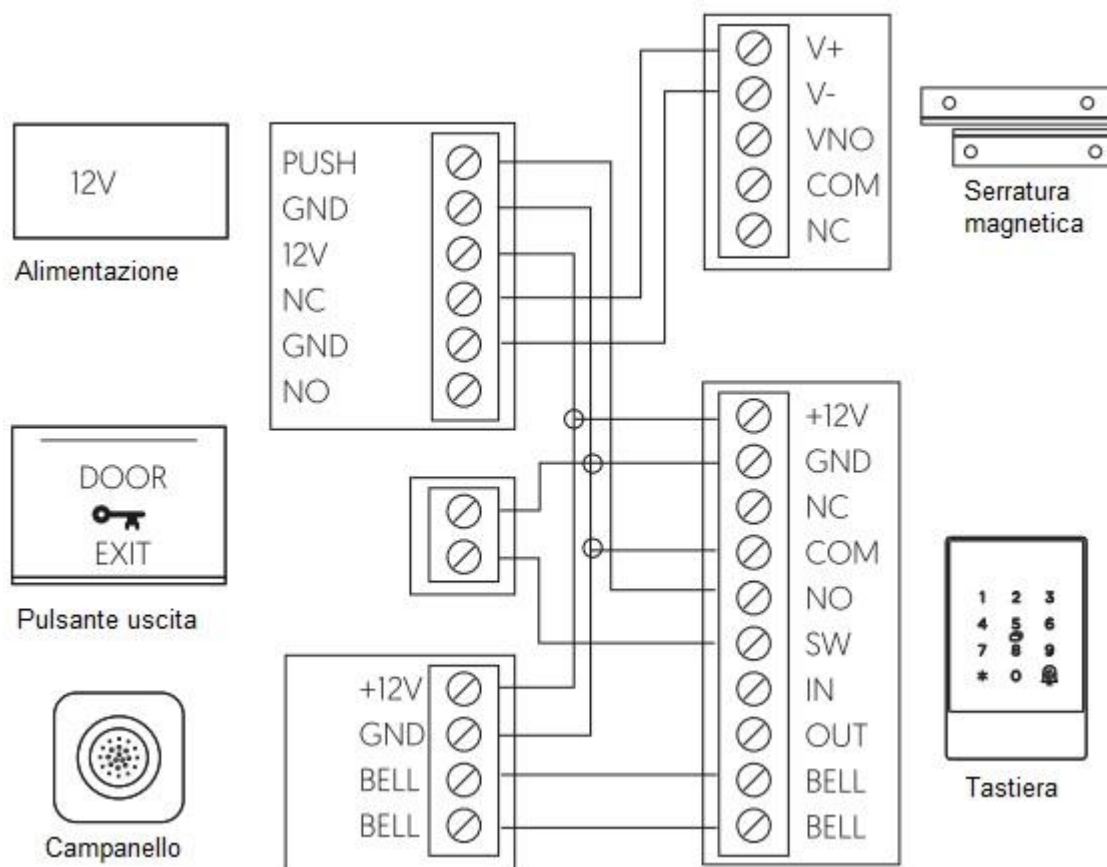


Fig. 2.4. Collegamenti BS200K

2.2 Gateway WiFi

Il Gateway è mostrato in Fig. 2.5.



NOTA.

Il Gateway deve essere installato in una posizione tale da poter accedere al Router WiFi del sito. Controllare la portata del segnale WiFi prima di scegliere la posizione del Gateway.

Il Gateway deve avere una distanza massima di 30 m circa dalle tastiere; tener presente che ostacoli (es. muri) riducono la portata del segnale Bluetooth.

In assenza di comunicazione wireless, le tastiere BS200K lavorano in stand-alone con i codici che hanno nella propria memoria: il gateway deve poter comunicare con le tastiere per aggiornare da remoto i codici PIN e/o le limitazioni di utilizzo delle credenziali di accesso.



Fig. 2.5. Gateway WiFi

Collegare il Gateway alla presa elettrica 230Vca mediante il cavetto USB e il caricabatterie da 5V @ 1A.

2.3 Maniglia FL200KCS

Per l'installazione della FL200KCS utilizzare le indicazioni dei seguenti documenti:

- https://drive.google.com/file/d/1Z6i02w4GVA3qip3tWcYKyinWd_dzsRX5/view?usp=sharing
- https://drive.google.com/file/d/1A8Y9oyxpAJCqTE3W2yZx0mZwg_xr2tl/view?usp=sharing



3 Programmazione del sistema

3.1 Download APP

Il sistema è gestito attraverso APP disponibili, senza alcun costo, negli store di Apple e Google. L'APP da scaricare e installare sul proprio dispositivo è "TTLOCK" e l'icona è mostrata in Fig. 3.1.

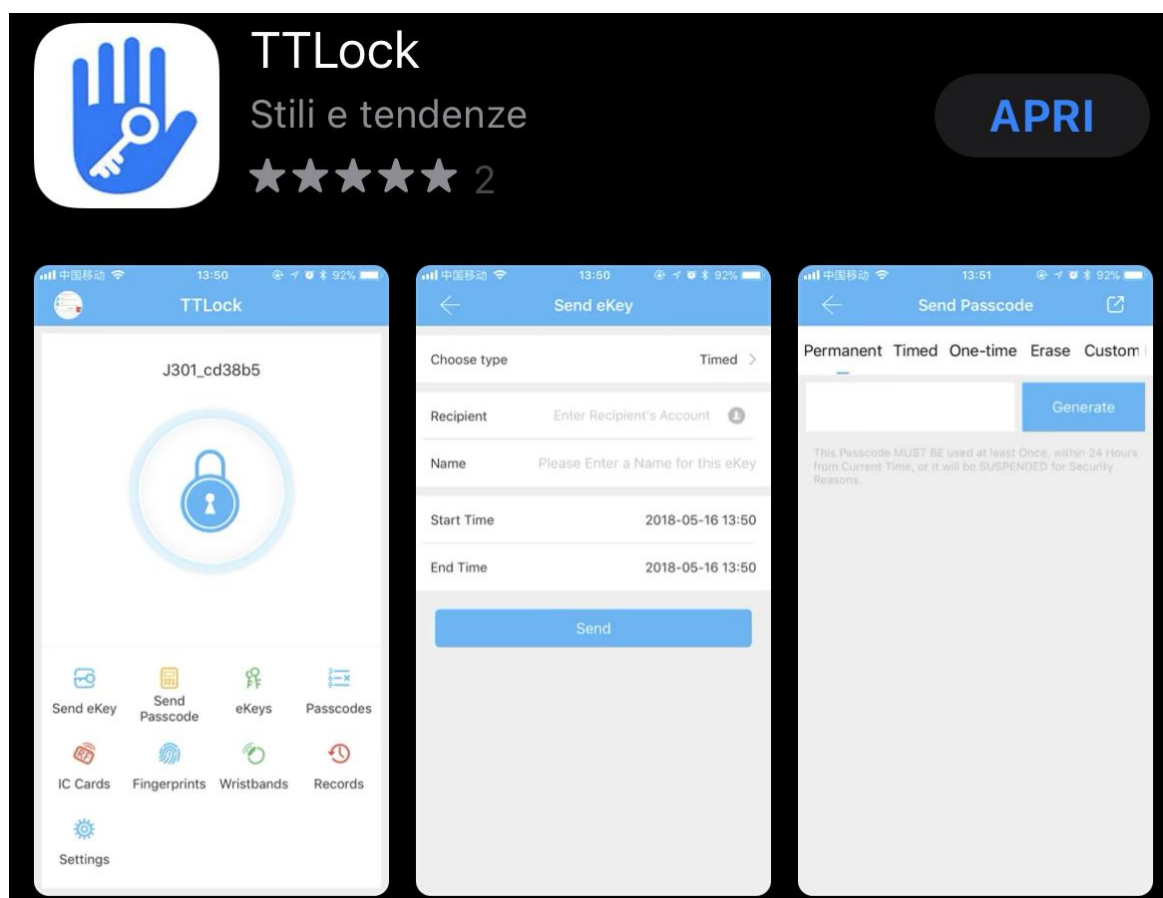


Fig. 3.1. Icona App TTLOCK

Eseguire l'installazione dell'APP sul proprio smartphone seguendo le indicazioni che il software fornisce: al termine dell'installazione, l'APP comparirà nell'elenco delle APP del proprio smartphone. Si consiglia di utilizzare l'App nella schermata home.



3.2 Account

All'apertura dell'APP viene richiesta la registrazione dell'account di amministratore: l'account può essere definito sia attraverso il numero di telefono della SIM dello smartphone (Fig. 3.2 a) che attraverso un indirizzo di posta elettronica (Fig. 3.2. b).

Per entrambe le registrazioni, la procedura è identica: il software chiede che venga scelto il Paese e quindi il relativo prefisso telefonico internazionale (nel caso dell'Italia il prefisso è +39), il numero di telefono della SIM, una password associata all'account (digitata due volte e con caratteristiche di robustezza per non essere facilmente clonata); confermando con "Ricevi Codice" viene inviato un codice OTP di verifica mediante SMS al numero di telefono indicato, codice che deve essere inserito nell'ultimo campo entro un minuto (il conteggio in secondi per il timeout compare nel riquadro accanto al codice di verifica). Analogamente, nel caso di inserimento di un indirizzo email, il codice OTP richiesto verrà inviato per posta elettronica.

Al termine, toccare il pulsante "Registrare" per accedere alle funzioni del software.

La procedura di login deve essere eseguita tutte le volte che l'APP viene chiusa: se l'account è stato creato con il numero di telefono, usare questo numero come "user" e digitare la password scelta. Altrimenti nel campo user inserire l'indirizzo di email.

The figure displays two screenshots of the account registration interface. Both screens feature a blue header with a back arrow, the 'Registrare' button, and status bar information (App Store, signal, time, battery). Below the header are two tabs: 'E-mail' and 'Telefono'.
Screenshot (a) shows the 'Telefono' tab selected. It includes a 'Paese / Regione' field set to 'Italy+39', a phone number field containing '335238046', a password field, and a verification code field. A 'Ricevi Codice' button is present. A note at the bottom states: 'La password deve contenere 8-20 caratteri e includere...'.
Screenshot (b) shows the 'E-mail' tab selected. It includes an email address field containing 'doingsecurity.gs@gmail.com', a password field, and a verification code field. A 'Ricevi Codice' button is present. A note at the bottom states: 'La password deve contenere 8-20 caratteri e includere almeno due tipi di numeri, lettere e simboli'.
Both screens feature a numeric keypad at the bottom for entering the verification code, with a 'Fine' button and a back arrow.

Fig. 3.2. Registrazione account: a) con numero di telefono, b) con indirizzo di email



3.3 Setup

Dopo il login toccare il pulsante di setup che si trova in alto a sinistra : si apre la schermata di Fig. 3.3 dove è possibile effettuare le diverse configurazioni dell'impianto.

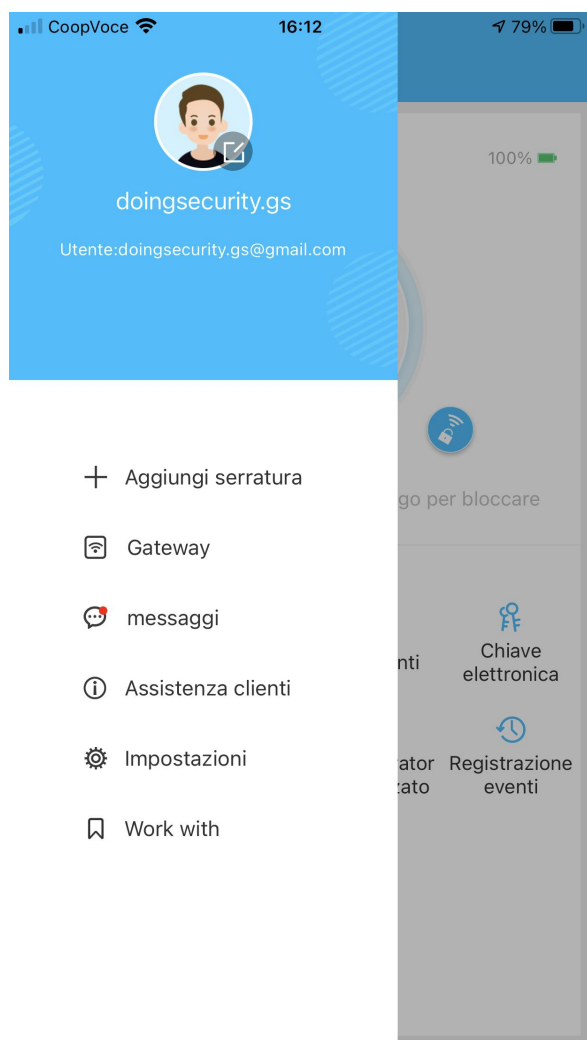


Fig. 3.3. Setup

3.4 Aggiunta Gateway, Tastiere e Serrature

Per prima cosa si deve collegare il Gateway dell'impianto al WiFi e aggiungere alla configurazione le tastiere presenti nel sistema.

Toccare la voce del menu di Setup "Gateway" e scegliere il tasto "+" in alto a destra: il software chiede che il Gateway venga collegato all'alimentazione e che si verifichi che il LED sia lampeggiante alternativamente in blu e rosso. Scegliere il tipo di Gateway (nel caso in esame il modello G2) - vd. Fig. 3.4.

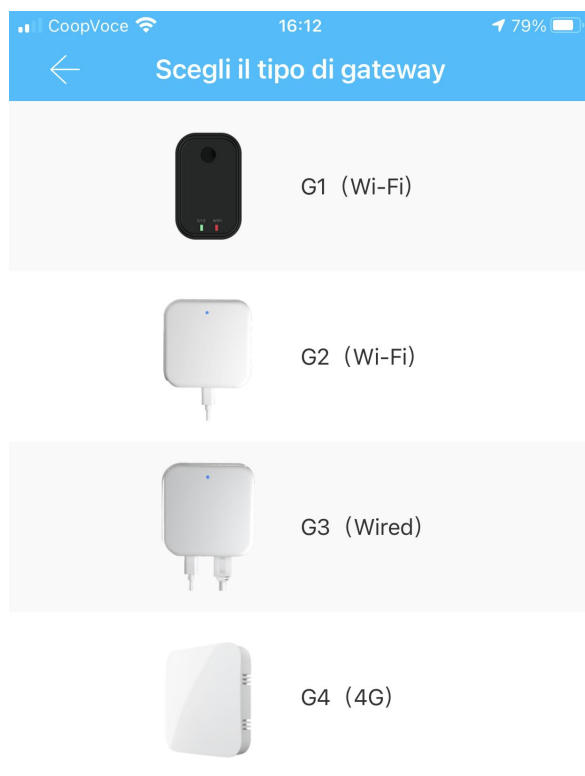


Fig. 3.4. Collegare Gateway

Il software ricerca la presenza di Gateway all'interno della rete WiFi a cui lo smartphone è collegato. Se il Gateway viene rilevato, compare nell'elenco dei Gateway con il livello di potenza del segnale WiFi.

Confermando con il tasto "+" il Gateway individuato attraverso il proprio codice ID preceduto dal tipo di prodotto (G2), lo si associa alla rete WiFi del proprio sito inserendo la password del router, fornendo un nome mnemonico al Gateway e infine toccando il pulsante "Ok" - vd. Fig. 3.5.

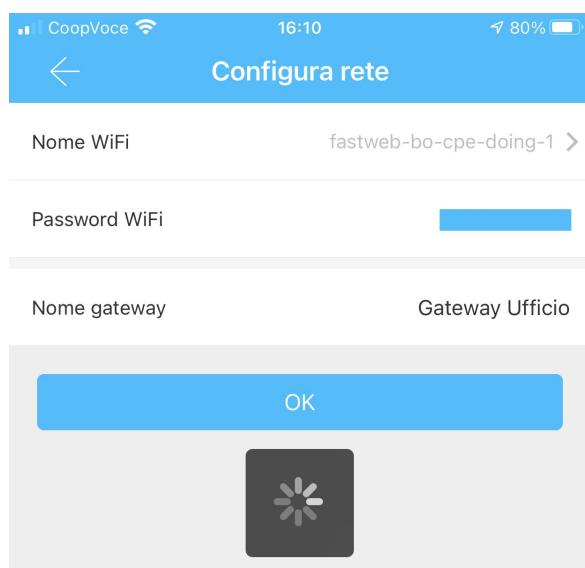


Fig. 3.5. Gateway associato alla rete WiFi



Il Gateway ora compare nell'elenco dei dispositivi appartenenti all'account - vd. Fig. 3.6.

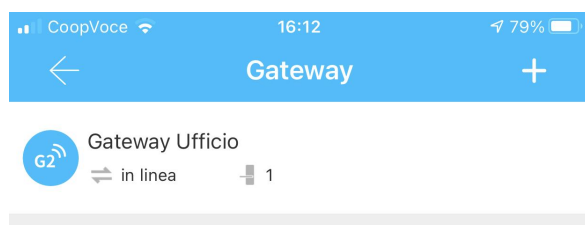


Fig. 3.6. Gateway nell'elenco dispositivi associati

Per aggiungere le tastiere all'impianto, toccare "+ Aggiungi serratura" a partire dal menu di Setup (vd. Fig. 3.3); si apre la schermata di Fig. 3.7.

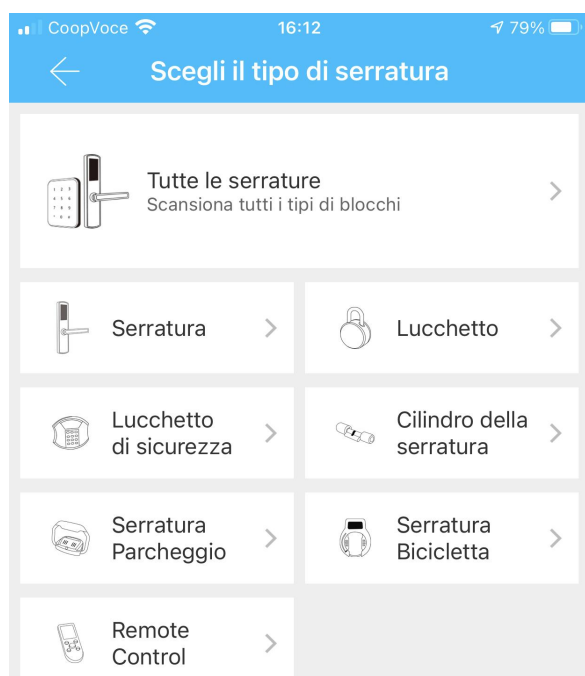
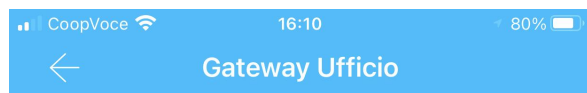


Fig. 3.7. Connessione serrature al Gateway

Utilizzare la prima voce "Tutte le serrature". La scansione delle serrature raggiunte dal segnale inviato dal Gateway (vd. Fig. 3.8) produce un elenco di dispositivi molto simile a quanto precedentemente visto per la scansione dei Gateway.



Le serrature in scansione
appartengono a te

Fig. 3.8. *Elenco serrature individuate dal Gateway*

La tastiera viene individuata con il proprio codice ID preceduto dal tipo di prodotto; toccando il pulsante “+” si aggiunge la tastiera all’impianto e le si attribuisce un mnemonico a scelta dell’utente - vd. Fig. 3.9. Notare che la potenza del segnale viene mostrata accanto all’icona e al nome attribuito alla tastiera.



Fig. 3.9. *Mnemonico associato alla serratura*

La configurazione dell’hardware dell’impianto è terminata quando tutte le tastiere / serrature sono aggiunte e rinominate all’interno del sistema.

3.5 Definizione PIN e Tessere RFID

A partire dalla schermata principale, si possono programmare codici PIN e Tessere RFID per eseguire le funzioni di controllo accessi - vd. Fig. 3.10.

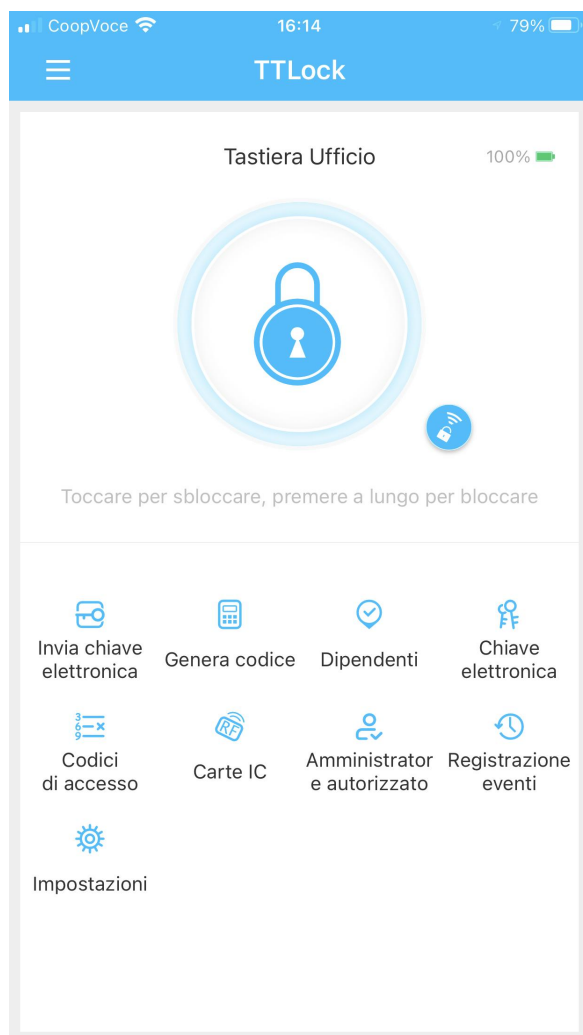


Fig. 3.10. Definizione credenziali di apertura

Per prima cosa verificare che toccando il simbolo “lucchetto” la serratura si sblocchi. La corretta esecuzione del comando è illustrata in Fig. 3.11.

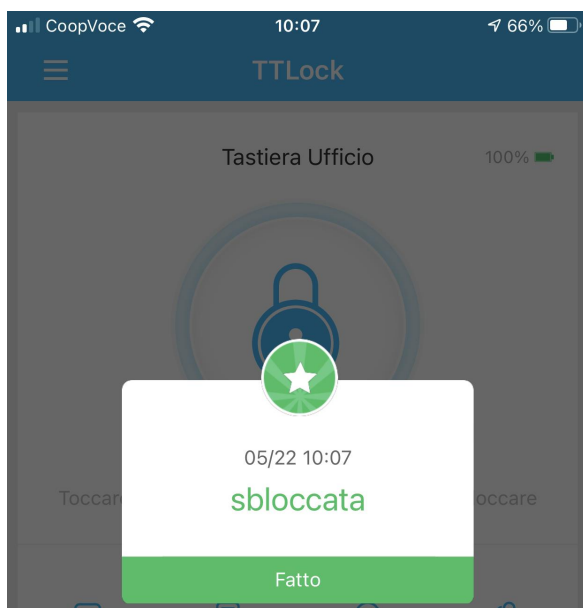


Fig. 3.11. Sblocco serratura con comando da APP (via Bluetooth)

Le funzioni eseguibili a partire dalla schermata di Fig. 3.10, sono:

- Inviare una chiave elettronica
- Generare un codice PIN
- Gestire le chiavi elettroniche
- Gestire i PIN di accesso
- Associare le tessere RFID alla serratura
- Editare il profilo dell'Amministratore
- Verificare il log degli eventi
- Aprire il menu di Impostazioni

3.5.1 Generare un codice PIN

Se si intende generare un codice PIN che possa essere poi inviato ad un ospite affinché possa usarlo in autonomia, toccare la funzione "Genera codice".

Il software chiede di specificare se il PIN è permanente, temporizzato, per un singolo accesso, ecc.

Viene chiesto un nome utente a cui il PIN verrà associato e - nel caso di PIN temporaneo - vengono proposte la data/ora di inizio validità e la data/ora di fine validità del PIN. Infine toccando il pulsante "Creare" si ottiene la generazione del PIN da parte del software. Vd. Fig. 3.12 a) e b).

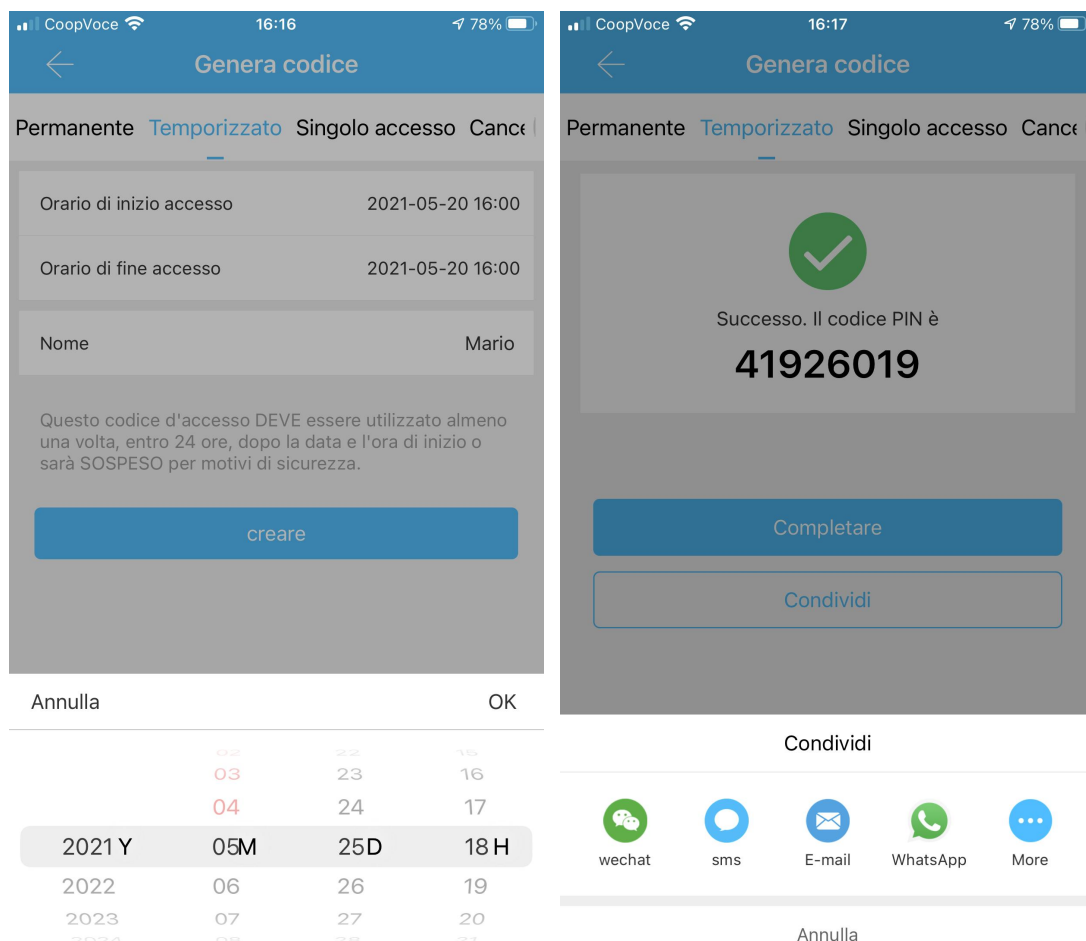


Fig. 3.12. (a) Crea codice PIN - (b) PIN generato dal software

Il codice PIN generato dal software può essere condiviso con un utente remoto affinché lo possa utilizzare quando previsto (pulsante "Condividi"). L'uso del PIN mostra nello smartphone dell'amministratore la notifica come mostrato in Fig. 3.13.

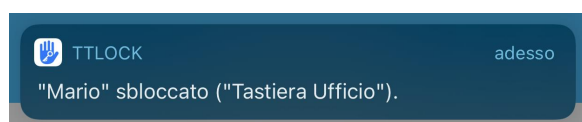


Fig. 3.13. Notifica di accesso PIN

3.5.2 Associare una tessera RFID

Se si intende associare una tessera RFID Mifare® classic 1k ad un utente, toccare l'icona "Carte IC" per ottenere la schermata di Fig. 3.14.

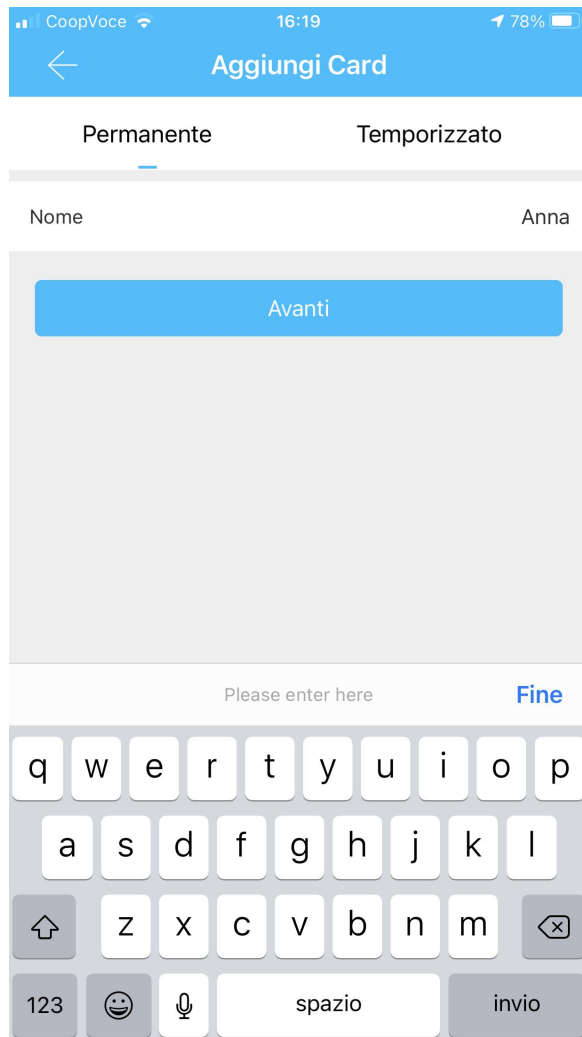


Fig. 3.14. Associazione tessera RFID all'utente

Per prima cosa scegliere se la tessera RFID è permanente o temporizzata, cioè con validità a partire da una data/ora fino ad una data/ora.

Quindi dopo aver fornito un nome utente da associare alla tessera RFID, toccare sul pulsante "Avanti" per avviare la procedura di abbinamento avvicinando la tessera RFID al lettore. L'elenco degli utenti che dispongono di tessere RFID associate è mostrato in Fig. 3.15; i tre puntini in alto a destra permettono di eseguire una gestione delle credenziali inclusa la cancellazione di un codice tessera.

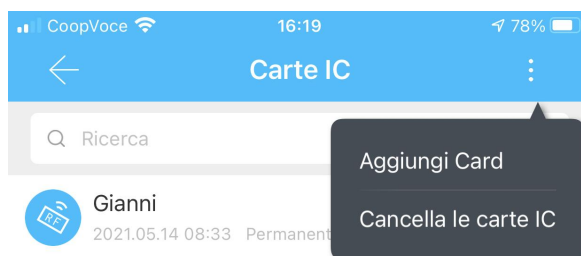


Fig. 3.15. Elenco utenti abbinati alle tessere RFID



Toccando su un nome utente, è possibile modificarne le credenziali e la validità dell'uso della tessera RFID - vd. Fig. 3.16.

The screenshot shows a mobile app interface with a blue header bar containing a back arrow, the title 'Informazioni sulla scheda IC', and status icons for signal, Wi-Fi, time (10:26), and battery (65%). Below the header, the user information is displayed in a list format:

Numero di carta	2045466367
Nome	Anna >
Periodo di validità	Permanente >
Operatore	doingsecurity.gs
Tempo	2021-05-20 16:19:40
Registrazione eventi	>

Below the list, there is a light gray rectangular button labeled 'Elimina'.

Fig. 3.16. *Modifica del profilo utente*

3.6 Log Accessi

A partire dalla schermata principale - vd. Fig. 3.10 - toccando "Registrazione eventi" si ottiene l'elenco dei log che il sistema ha generato (vd. Fig. 3.17). L'amministratore è così in grado di verificare il corretto utilizzo del sistema.

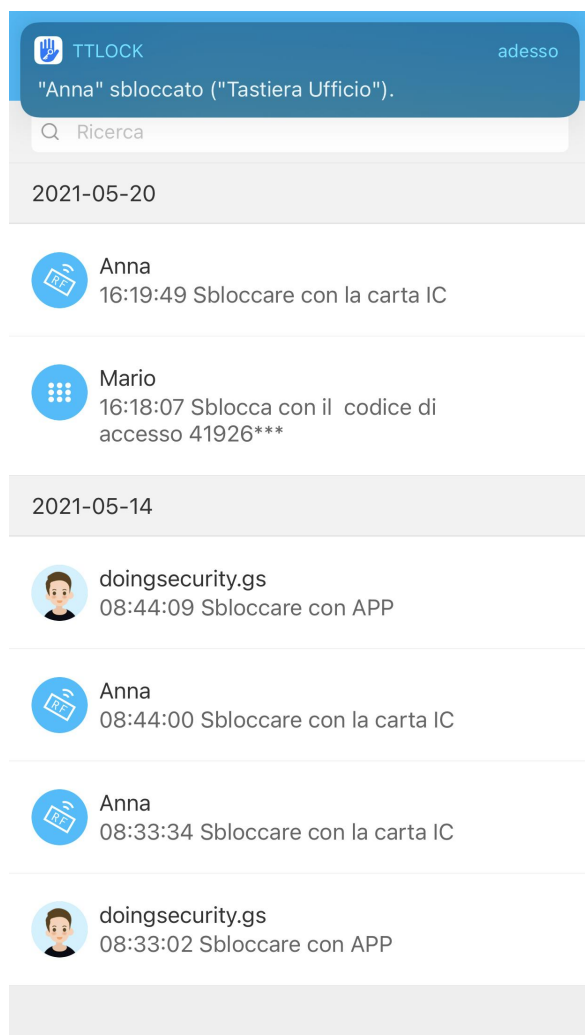


Fig. 3.17. *Registrazione eventi*

3.7 Funzioni Avanzate

A partire dalla schermata di setup - vd. Fig. 3.3 - toccando "Impostazioni" si ottiene l'elenco delle funzioni mostrate in Fig. 3.18.

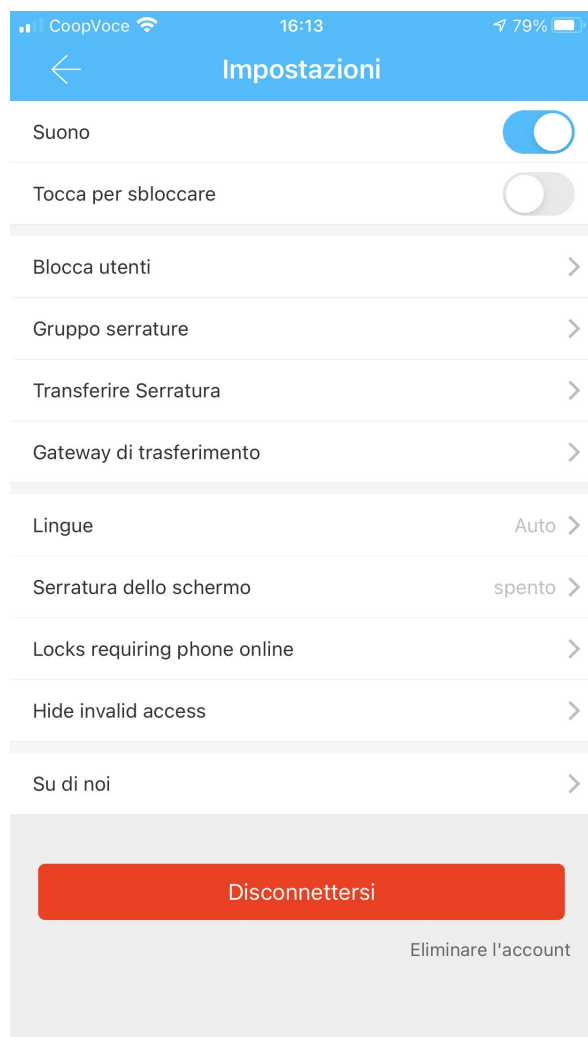


Fig. 3.18. *Impostazioni avanzate*

Fra le impostazioni di questa pagina, è interessante far notare la funzione di trasferimento di una tastiera / serratura da un impianto ad un altro.

Qualora una tastiera / serratura dovesse essere eliminata dall'impianto, ricordarsi che l'eliminazione va confermata utilizzando la stessa password di amministratore come precedentemente illustrato. **Una tastiera che non fosse eliminata da una configurazione, rimarrebbe inutilizzabile in altri impianti.**

3.8 Opzioni

Molti B&B richiedono un controllo dei carichi elettrici per ciascuna stanza (es. Condizionatori, Televisori, ...), così da prevenire la dimenticanza di apparati accesi qualora l'ospite non fosse più presente nella stanza. DoingSecurity propone uno switch elettronico con tasca porta-badge per tessere Mifare® che è in grado di commutare 30A: è quindi in grado di attivare / disattivare il Q.E presente nella camera dell'ospite. Per far sì che l'ospite sia tenuto a usare la tessera prelevandola dallo switch, è possibile assegnare all'ospite un PIN per un singolo accesso e fargli trovare nella camera il badge inserito nella tasca porta-badge assieme alle istruzioni di uso della tastiera con RFID dopo il primo utilizzo.