TR210F / TR210WIFIF / TR210BTF (Mifare)
TR210EF / TR210WIFIEF / TR210BTEF (EM 125KHz)
Terminale di controllo accessi stand alone con lettore di impronte digitali

Manuale di programmazione

ATTENZIONE

Se stai utilizzando il terminale TR210 senza lettore di impronta digitale, questo NON è il manuale corretto.

Il TR210 è un dispositivo multifunzionale per il controllo degli accessi di un varco, progettato per adattarsi a diverse esigenze operative. Può essere utilizzato sia come controllore autonomo (stand-alone) sia come semplice lettore e tastiera compatibile con il protocollo Wiegand.

Il dispositivo è in grado di memorizzare fino a 1.000 utenti, con un massimo di 100 impronte digitali, tra cui 2 utenti speciali designati come “coercizione” e 10 utenti temporanei per i visitatori. Supporta diverse modalità di riconoscimento, tra cui:

- Impronta digitale
- Carta
- PIN
- Carta + PIN (Non disponibile nella versione WiFi)
- Multi-carta, con o senza l'uso del PIN.

Oltre alle funzioni di base, il TR210F offre una serie di funzionalità avanzate, come l’interblocco tra due porte, un ingresso Wiegand, e altre opzioni che vengono descritte nel dettaglio nelle sezioni successive di questo manuale. **TR210F** legge le carte Mifare, **TR210EF** le carte EM a 125KHz.

Versioni disponibili

Lettore Mifare		**Lettore EM 125KHz**	
Modello	Comunicazione	Modello	Comunicazione
TR210F	-	TR210EF	-
TR210BTF	Bluetooth	TR210BTEF	Bluetooth
TR210WIFIF	WiFi	TR210WIFIEF	WiFi

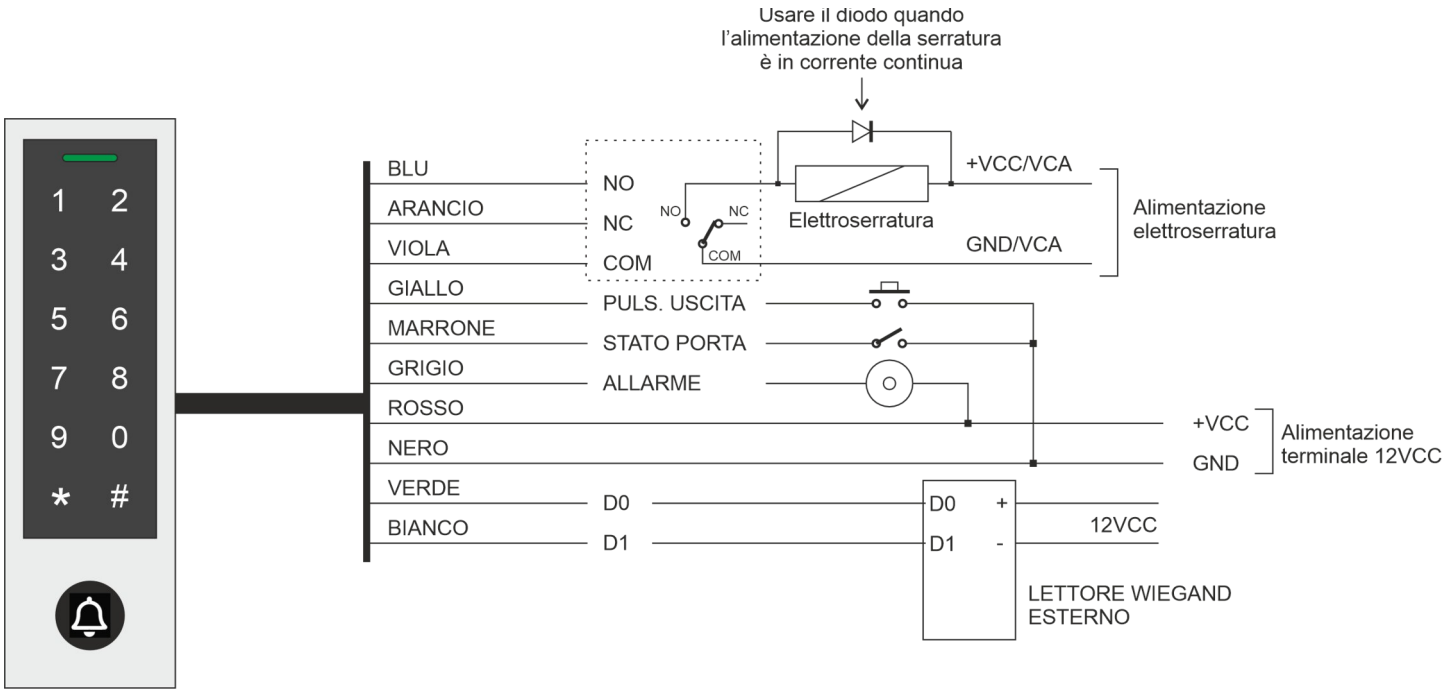
I modelli Bluetooth e WiFi possono essere gestiti attraverso l’app TUYA che consente:

- Gestione fino a 500 utenti anche indicando data e ora di validità e scadenza
- Visualizzare lo storico degli eventi
- Ricevere una notifica a seguito della pressione del campanello
- Verificare lo stato della porta
- Comandare l’apertura da remoto

Il modello WiFi permette la gestione remota da qualsiasi luogo coperto da internet, mentre il modello Bluetooth ha la comodità della programmazione via app ma richiede di essere nelle vicinanze del dispositivo.

Connessioni in modalità controller

Lo schema rappresenta le connessioni da effettuare in **modalità controller**, cioè quando il dispositivo si occupa di verificare la validità della tessera o del codice digitato e comanda il varco in caso di credenziali valide. La modalità controller è quella programmata di default dalla fabbrica.



- E' sempre raccomandato di separare l'alimentazione del terminale da quella della serratura, utilizzando due distinti alimentatori.
- Se la serratura è alimentata in corrente continua, inserire in parallelo alla serratura un diodo col catodo (lato della fascetta) rivolto verso il potenziale positivo.
- Qualora la serratura fosse alimentata a 12VDC e volessimo utilizzare un unico alimentatore, raccomandiamo di sovradimensionarlo per poter sopportare il picco di assorbimento della corrente di spunto della elettro serratura senza interferire con l'elettronica del controller
- E' possibile collegare un pulsante per la richiesta di uscita, il contatto stato porta, un ripetitore di allarme e anche un lettore ausiliario che potrebbe essere installato dal lato esterno a minor sicurezza in modo da mantenere l'elettronica ed il relè di apertura all'interno.

Confgurazione tramite APP:

I dispositivi con WIFI o Bluetooth possono essere configurati sia localmente, utilizzando la tastiera e la carta master, sia con APP TUYA. In questo caso, per prima cosa, scaricare l'APP "Tuya Smart" dallo store.

"***Tuya Smart***"

ANDROID **IOS**

Una volta installata l'APP devi creare un account utilizzando una email valida che ti sarà utile per un eventuale recupero password. Quindi **assicurati che il tuo smartphone sia connesso alla stessa rete WiFi a cui vorrai connettere il controller**, alimenta il controller e clicca l'icona + in alto a destra sull'APP per aggiungere il dispositivo. L'APP troverà il dispositivo e segui la procedura guidata per completare l'operazione. Attenzione: il dispositivo funziona su una rete WiFi a 2,4GHz.

Se il dispositivo non venisse trovato è necessario resettare la configurazione di rete (WiFi o Bluetooth) digitando la seguente sequenza:

```
* [Codice master] #9 [Codice master] # *
```

Se è stato smarrito il codice master, vedere il capitolo per resettare il dispositivo alla configurazione di fabbrica.

Cos'è l'APP TUYA Smart?

TUYA Smart è un'applicazione di terze parti selezionata per la configurazione e il controllo del prodotto. L'app non è sviluppata né gestita dalla nostra azienda: le sue funzionalità potrebbero essere aggiornate o modificate senza preavviso, pertanto non possiamo garantirne la documentazione puntuale né assumere responsabilità per eventuali malfunzionamenti.

Gestione utenti con APP Tuya

Mediante l'APP potrai aggiungere utenti e assegnargli carte RFID e/o codici PIN. Potrai stabilire un periodo di validità da data/ora a data/ora e anche assegnare una eventuale fascia oraria in cui l'accesso è permesso, creare codici temporanei validi solo per un certo numero di passaggi e molto altro. L'APP è molto intuitiva e permette una gestione semplice del dispositivo. L'app ti permetterà anche di visualizzare gli eventi o le anomalie.

Alcune configurazioni iniziali saranno invece fatte mediante programmazione locale prima di iniziare a gestire il prodotto esclusivamente da APP.

Programmazione da tastiera (senza app)

- Per entrare in programmazione si digiti:

```
* [Codice master] #
```

- Per uscire dalla programmazione si digiti:

```
*
```

Il Codice master di programmazione è 123456, si raccomanda di modificarlo come spiegato qui di seguito.

Modificare il Codice Master – RACCOMANDATO -

```
* [Codice master] # 0 [Nuovo codice master] # [Nuovo codice master] # *
```

Impostare la modalità di lavoro:

- Modalità controller (default):

```
* [Codice master] # 7 7 # *
```

- Modalità lettore:

```
* [Codice master] # 7 8 # *
```

Modalità controller

Aggiungi utenti:

Cos'è l'ID utente?

Non è obbligatorio, ma è possibile tenere traccia del numero progressivo di registrazione che chiameremo "**ID Utente**". Grazie all' ***ID utente*** sarà possibile:

- Eliminare facilmente le credenziali anche in caso di smarrimento o indisponibilità della credenziale RFID, ad esempio se la carta è stata smarrita.
- Assegnare un codice PIN allo stesso utente possessore di credenziale RFID.

Nel caso in cui non venissero utilizzate credenziali RFID, ma solo codici PIN, la cancellazione del singolo utente avverrà tramite codice PIN e in quel caso non sarà necessario tenere traccia dell' ***ID Utente***.

Aggiungi impronta digitale:

- ***ID Utente*** automatico:

```
* [Codice master] # 1 [Leggi impronta 3 volte]
```

  Le impronte possono essere aggiunte in modo continuo, ogni 3 letture un utente.

- Seleziona ***ID Utente***:

```
* [Codice master] # [ID Utente] # [Leggi impronta 3 volte]
```

  Le impronte possono essere aggiunte in modo continuo, ogni 3 letture un utente. Gli ID utenti con impronta havranno ID compreso tra 0 e 98.

Aggiungi credenziale RFID:

- ***ID Utente*** automatico:

```
* [Codice master] # 1 [leggi la carta o digita il codice a 8/10/17 cifre] #
```

  Le carte possono essere aggiunte continuamente, alla fine premere * per terminare.

- Seleziona ***ID Utente***:

```
* [Codice master] # 1 [ID Utente] # [leggi la carta o digita il codice a 8/10/17 cifre] # *
```

  Nota: gli ID utente validi vanno da 100 a 987.I codici da 988 a 989 sono riservati per la coercizione e i codici da 990 a 999 per i visitatori.

Aggiungi PIN:

- ***ID Utente*** automatico:

```
* [Codice master] # 1 [Digita PIN] #
```

I codici PIN possono essere aggiunte continuamente, alla fine premere * per terminare.

- Seleziona ***ID Utente***:

```
* [Codice master] # 1 [ID Utente] # [PIN] # *
```

I codici PIN possono essere qualsiasi numero di 4, 5 o 6 cifre ad esclusione di 8888 che è riservato.

Sicurezza PIN, valido solo per codici a 6 caratteri:

Per confutare la digitazione del PIN, l'utente può aggiungere 2 caratteri prima e anche 2 caratteri dopo al suo PIN a 6 cifre. Esempio col pin 123456 posso digitare 43**123456**97 oppure 87**123456**.

Aggiungi codici di coercizioni:

Aggiungere credenziale RFID oppure codice PIN utilizzando la procedura con selezione dell' ID Utente numero 988 e 989. Presentando una credenziale RFID di coercizione o digitando il PIN si otterrà l'apertura della porta e l'attivazione dell'uscita di allarme.

Aggiungi codici visitatori:

I codici visitatori sono credenziali (RFID o PIN) valide per 1...10 ingressi. Si memorizzano utilizzando i 10 ID Utente che vanno da 990 a 999. Il numero accessi può essere configurato da 0 a 9, 0 significa 10 accessi.

- Credenziale RFID:

```
* [Codice master] # 1 [ID Utente] # [numero accessi] # [leggi carta] # *
```

- Codice PIN:

```
* [Codice master] # 1 [ID Utente] # [numero accessi] # [PIN] # *
```

Modifica PIN:

Questa operazione potrà essere compiuta anche dall'utente stesso, quindi senza utilizzare il master code. Deve però essere conosciuto l' ***ID Utente***.

```
* [ID Utente] # [Vecchio PIN] # [Nuovo PIN] # [Nuovo PIN] # *
```

Cancella utenti:

- Ho la carta o conosco il PIN o anche l'utente con la sua impronta:

```
* [Codice master] # 2 [Leggi carta oppure digita PIN oppure leggi impronta] #
```

Gli utenti possono essere cancellati continuamente, alla fine premere * per terminare.

- Conosco l'ID Utente:

```
* [Codice master] # 2 [ID Utente] # *
```

- Conosco il codice carta:

```
* [Codice master] # 2 [Codice carta a 8/10/17 cifre] # *
```

Cancella tutti gli utenti:

```
* [Codice master] # 2 [Codice master] # *
```

Configura il relè:

- Impulsivo (default 5 sec.):

```
* [Codice master] # 3 [Tempo in secondi 1-99] # *
```

- Passo-passo:

CE

```
* [Codice master] # 3 0 #
```

Modalità di accesso:

- Accesso solo con impronta digitale:

```
* [Codice master] # 4 0 # *
```

- Accesso solo con carta:

```
* [Codice master] # 4 1 # *
```

- Accesso solo con PIN:

```
* [Codice master] # 4 2 # *
```

- Accesso con carta + PIN (Non supportato dal modello WiFI)

```
* [Codice master] # 4 3 # *
```

- Accesso con carta o con PIN o con impronta:

```
* [Codice master] # 4 4 # *     (default)
```

- Accesso multi utente:

```
* [Codice master] # 4 3 [2...9 utenti] # *
```

In modalità multi-utente, la porta sarà aperta solo dopo la verifica di 2...9 credenziali valide.

Blocco su errori consecutivi:

E' possibile bloccare il terminale per 10 minuti e attivare l'allarme a seguito di N tentativi di accesso negati. Sebbene bloccato, il terminale permetterà sempre di aprire la porta utilizzando il pulsante di richiesta di uscita.

- Disabilita (default):

```
* [Codice master] # 6 0 # *
```

- Abilita

```
* [Codice master] # 6 1 # *
```

- Tempo di allarme:

```
* [Codice master] # 6 2 # 5 [1...3 minuti] # *      (default 1 minuto)
```

Stato porta:

E' possibile attivare lo stato porta per avere un allarme quando questa viene forzata (aperta senza utilizzare le credenziali o il pulsante di uscita) e anche se rimane aperta per oltre 1 minuto.

- Disabilita:

```
* [Codice master] # 6 3 # *
```

- Abilita + tempo allarme:

```
• * [Codice master] # 6 4 # 5 [1...3 minuti] # *      (default 1 minuto)
```

Questo tempo sarà il medesimo dell'allarme tamper

Risposta sonora e luminosa:

- Disabilita buzzer:

```
* [Codice master] # 7 0 # *
```

- Abilita buzzer:

```
* [Codice master] # 7 1 # * (default)
```

- Disabilita LED:

```
* [Codice master] # 7 2 # *
```

- Abilita LED:

```
* [Codice master] # 7 3 # * (default)
```

- Disabilita retroilluminazione:

```
* [Codice master] # 7 4 # *
```

- Abilita retroilluminazione:

```
* [Codice master] # 7 5 # *
```

- Abilita retroilluminazione automatica:

```
* [Codice master] # 7 6 # * (default)
```

La retroilluminazione automatica si spegne dopo 20 secondi di inattività e si accende alla pressione del primo tasto che non verrà preso in considerazione come tasto digitato.

Registra impronta master:

```
* [Codice master] # 1 9 9 # [Leggi impronta 3 volte] *
```

Utilizzo della carta o impronta master:

Per semplificare le operazioni di aggiunta impronta, carta o PIN (senza usare l' ID Utente esplicito), è possibile utilizzare una carta o l'impronta master.

- Aggiungi impronta digitale usando la carta o impronta master:

```
[Carta/impronta master] [impronta utente 1 (x3)] [impronta utente 2 (x3)] […]
[Carta/impronta master]
```

- Aggiungi credenziale RFID usando la carta o impronta master:

```
[Carta/impronta master] [Carta utente 1] [Carta utente 2] […] [Carta/impronta master]
```

- Aggiungi PIN:

```
[Carta/impronta master] [PIN 1 #] [PIN 2 #] […] [Carta/impronta master] (Digitare # dopo
ciascun PIN)
```

E' possibile utilizzare la carta o impronta master anche per cancellare gli utenti. Passarla 2 volte entro 5 secondi.

- Cancella impronta:

```
[Carta/impronta master 2 volte] [Impronta utente 1] [ Impronta utente 2] […]
[Carta/impronta master]
```

- Cancella credenziale RFID:

```
[Carta/impronta master 2 volte] [Carta utente 1] [Carta utente 2] […] [Carta/impronta
master]
```

- Cancella PIN:

```
[Carta/impronta master 2 volte] [PIN 1 #] [PIN 2 #] […] [Carta master]  (Digitare # dopo
ciascun PIN)
```

Cancellare l’allarme:

- Digitare il Codice Master seguito da #
- Passare la Carta Master
- Passare una credenziale valida o digitare un PIN valido seguito da #

Reset ai valori di fabbrica e aggiunta della Carta Master:

- Disalimentare il terminale se alimentato.
- Premere il pulsante di richiesta di uscita, mantenerlo premuto e alimentare il terminale
- Si udiranno 2 beep, rilasciare il pulsante e il LED diventerà giallo.
- Passare adesso una carta RFID che diventerà la Carta Master.

Notare che:

- Per eliminare la carta master memorizzata, dopo la procedura descritta sopra, anziché passare la carta master premere nuovamente il pulsante di richiesta di uscita e mantenerlo premuto per almeno 5 secondi.
- Il reset a default non elimina la lista degli utenti, ma ripristina tutti i parametri. Per cancellare la lista utenti seguire la procedura descritta nel paragrafo “Cancella tutti gli utenti”.
- Il reset a default non disassocia il dispositivo dalla rete WiFi o dal bluetooth dello smartphone dove era stato precedentemente registrato. Per poter registrare il dispositivo su una nuova app, digitare:

```
* [Codice master] #9 [Codice master] # *
```

Lettore esterno:

Un lettore esterno con uscita wiegand può essere connesso al terminale. Per selezionare il corretto formato da leggere utilizzare il seguente comando:

- Per carte EM:

```
* [Codice master] # 8 [digitare numero compreso tra 26 e 44 (bits)] # *
```

- Per carte Mifare:

```
* [Codice master] # 8 [da 26 a 44 o 56 o 58 (bits)] # *
```

In funzione del lettore utilizzato può occorrere disabilitare il controllo di parità. Ad esempio per leggere i formati 32, 40 o 56 bit è necessario disabilitarla.

- Disabilitare controllo di parità

```
* [Codice master] # 8 0 # *
```

- Abilitare controllo di parità

```
* [Codice master] # 8 1 # *
```

In modalità di programmazione sarà possibile aggiungere tessere utilizzando anche dal lettore esterno.

Tenere presente che il terminale non ha uscite per comandare il LED e il buzzer del lettore esterno. Se si desidera avere un feedback sonoro/luminoso, anziché pilotare l’elettro-serratura direttamente con lo scambio del relè interno, utilizzare un relè esterno a due scambi, uno per pilotare la serratura, l’altro per il pilotaggio dei segnali LED e buzzer del lettore.

Modalità speciale di acquisizione carte

Programmando questa modalità, il TR210 consentirà l'accesso a qualsiasi carta che sarà presentata, ovviamente con tecnologia compatibile. Allo stesso momento, le carte autorizzate saranno anche salvate in memoria.

- Abilita modalità acquisizione carte

```
* [Codice master] # 9 3 # *
```

- Disabilita modalità acquisizione carte

```
* [Codice master] # 9 2 # *
```

Modalità lettore

Formato wiegand di uscita:

- Per carte EM:

```
* [Codice master] # 8 [26...44 bit] # * (default 26 bit)
```

- Per carte Mifare:

```
* [Codice master] # 8 0 [26...44, 56, 56 bit] # * (default 34 bit)
```

- Formato wiegand digitazione tasti:

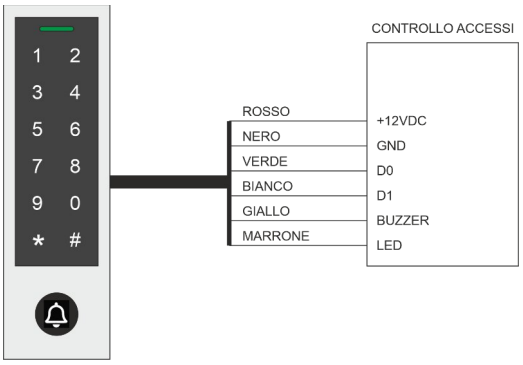
```
* [Codice master] # 8 [4, 8 o 10 bit] # * (default 4 bit)
```

- Disabilita parità:

```
* [Codice master] # 8 0 # *
```

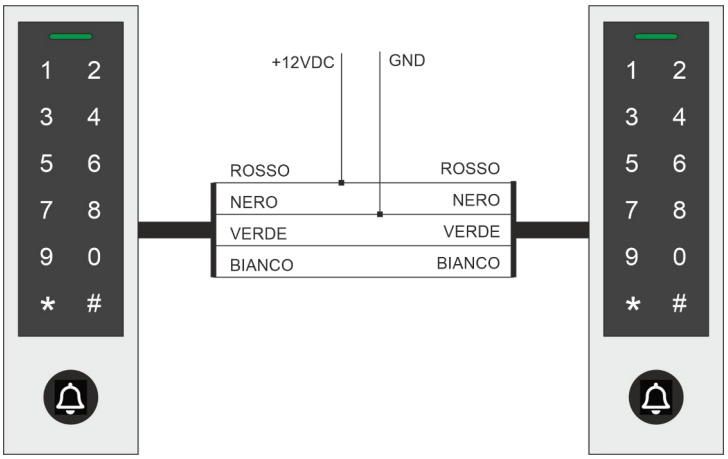
- Abilita parità:

```
* [Codice master] # 8 1 # * (default)
```



Lo schema di fianco mostra le connessioni tra il TR210 e un controller di accessi quando il TR210 è utilizzato in modalità lettore.

Copiare la programmazione degli utenti



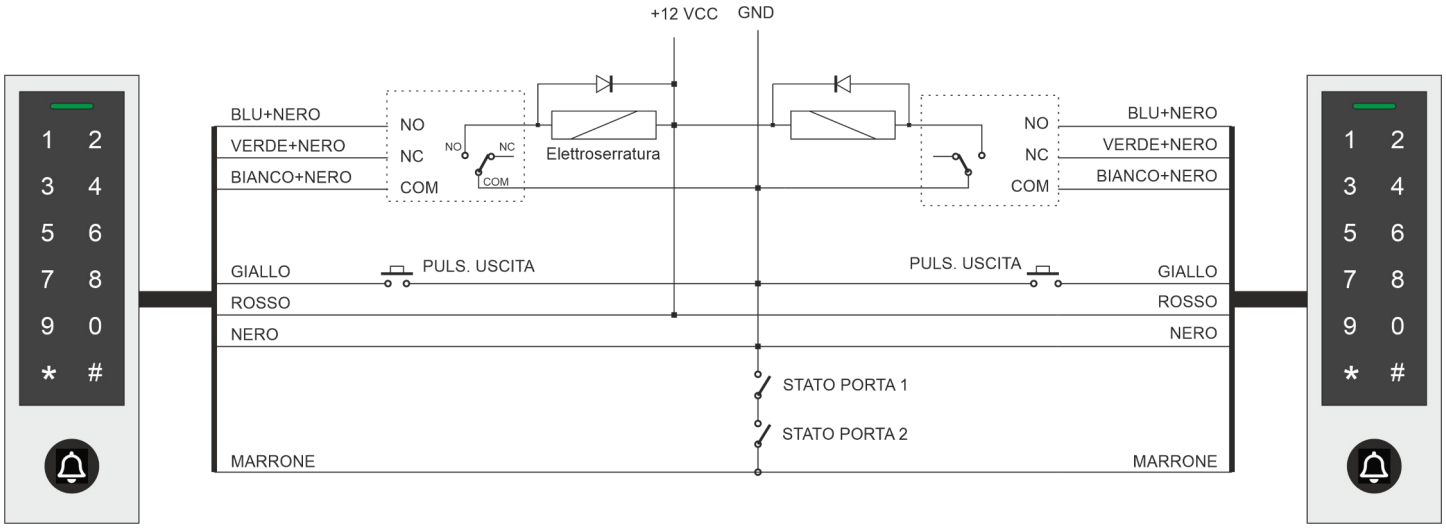
Per trasferire la lista utenti da un dispositivo (che chiameremo Master) ad un altro (che chiameremo Slave), collegarli come in figura e poi sul master digitare:

```
* [Codice master] # 9 8 #
```

Il led lampeggerà verde per indicare l'operazione in corso, al termine diventerà rosso, quindi digitare * per concludere l'operazione

Interblocco:

Per due porte interbloccate, utilizzare due terminali, collegando i due fili marroni assieme e i contatti di stato porta normalmente chiusi in serie, come nello schema semplificato sottostante.



La lista degli utenti abilitati può essere trasferita utilizzando la procedura descritta al paragrafo precedente, quindi su entrambi i dispositivi occorre abilitare la modalità di interblocco con il seguente comando:

- Abilita interblocco:

```
* [Codice master] # 9 1 # *
```

- Disabilita interblocco:

```
* [Codice master] # 9 0 # *     (default)
```