BIO CTRL SF1

Manuale utente

Versione 2.0, Luglio 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 BIO CTRL SF1 è l'evoluzione del BIO CONTROL - presente nella gamma DoingSecurity dal 2007.

La versione SF1 è stata aggiornata e migliorata nelle prestazioni e nelle capacità applicative, pur mantenendo il sensore ottico della precedente versione.

Il BIO CTRL SF1 dispone di un corpo metallico che lo rende adatto ad un maggior numero di applicazioni, incluso l'utilizzo in esterno. Il sensore rimane sempre protetto e, come sola manutenzione, necessita di rimanere pulito per poter permettere le letture delle impronte in tecnologia ottica.

Il lettore BIO CTRL SF1 mantiene del precedente modello le modalità operative stand-alone e con connessione in Wiegand ad un host di terze parti. Inoltre integra un lettore di prossimità EM 125 kHz.

Il presente Manuale descrive le diverse operazioni di programmazione e attivazione 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 o per altri motivi.

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 prodotto, seguire le istruzioni riportate di seguito:

- Controllare la tensione di alimentazione prima di collegare l'apparecchio alla rete o a tensioni non accettate dal prodotto
- Assicurare che l'installazione sia eseguita da un tecnico qualificato, nel rispetto di tutte le normative locali
- Installare interruttori di protezione per la linea di alimentazione dell'apparecchio e UPS o batterie di back-up, se richiesto dall'applicazione
- Utilizzare cablaggi in funzione delle condizioni di reale necessità del sito dove dovrà essere installato l'apparecchio (far riferimento al progetto dell'impianto elettrico)
- Per evitare danni accidentali, garantire un adeguato posizionamento del prodotto e - ove richiesto - adeguate condizioni di uso ambientale (far riferimento ai limiti di temperatura e umidità)
- Non aprire l'apparecchio: se il prodotto risultasse non funzionante in modo corretto, contattare il fornitore ai numeri riportati all'inizio del documento.

1.2 Organizzazione del presente manuale

Il presente Manuale Utente è diviso in sezioni. Il capitolo "**Descrizione del lettore**" fornisce le principali caratteristiche del prodotto, mentre il capitolo "**Installazione del lettore**" descrive come effettuare il corretto posizionamento meccanico del prodotto. Infine il capitolo "**Programmazione del lettore**" fornisce gli elementi per l'utilizzo del lettore nel primo utilizzo e nell'uso quotidiano.

1.3 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.
- **EPC Class1 Gen2** è lo standard di comunicazione “Electronic Product Code” per dispositivi che dialogano a frequenze comprese tra 860 e 950 MHz (nella banda Ultra High Frequency), inserito nello standard ISO/IEC 18000-6 Type C.
- **FHSS**, Frequency Hopping Spread Spectrum, tipo di modulazione a banda passante.

2 Descrizione del lettore

Il lettore BIO CTRL SF1 (o brevemente SF1) è un lettore di impronte digitali con housing metallico da esterno e lettore di prossimità EM 125 kHz integrato. La classe di protezione IP66 e il corpo anti-vandalico rendono il lettore utilizzabile in esterno.

Grazie al design sottile può essere facilmente installato sui profili porta.

NOTA.

Pur essendo IP66, il lettore SF1 ha un sensore ottico per la lettura delle impronte che deve essere mantenuto sempre pulito e asciutto perché possa leggere le impronte degli utenti.

Se il lettore SF1 venisse installato su superfici metalliche, far attenzione che la portata di lettura delle tessere 125 kHz può risultare fortemente compromessa: ove la funzione RFID fosse richiesta, tenere per quanto possibile la superficie di posa lontano dal lettore interponendo basette in materiale non-conduttivo (plastica, legno, ...).

Il lettore SF1 ha una memoria per 1000 impronte e 2000 tessere. L'output Wiegand permette di trasmettere i dati univoci degli identificativi utente in modalità 26 ~ 44 bit: può quindi essere collegato ad un qualsiasi controller di terze parti.

Infine il lettore BIO CTRL SF1 è equipaggiato con un ricevitore a infrarossi per le operazioni di programmazione e di acquisizione delle impronte digitali: l'operazione di acquisizione può essere anche fatta attraverso due tessere MASTER fornite nella confezione del prodotto, una per l'aggiunta di impronte in memoria e una per la cancellazione delle memorie.

Il contenuto della confezione del prodotto con gli accessori forniti è mostrato in Fig.2.1.

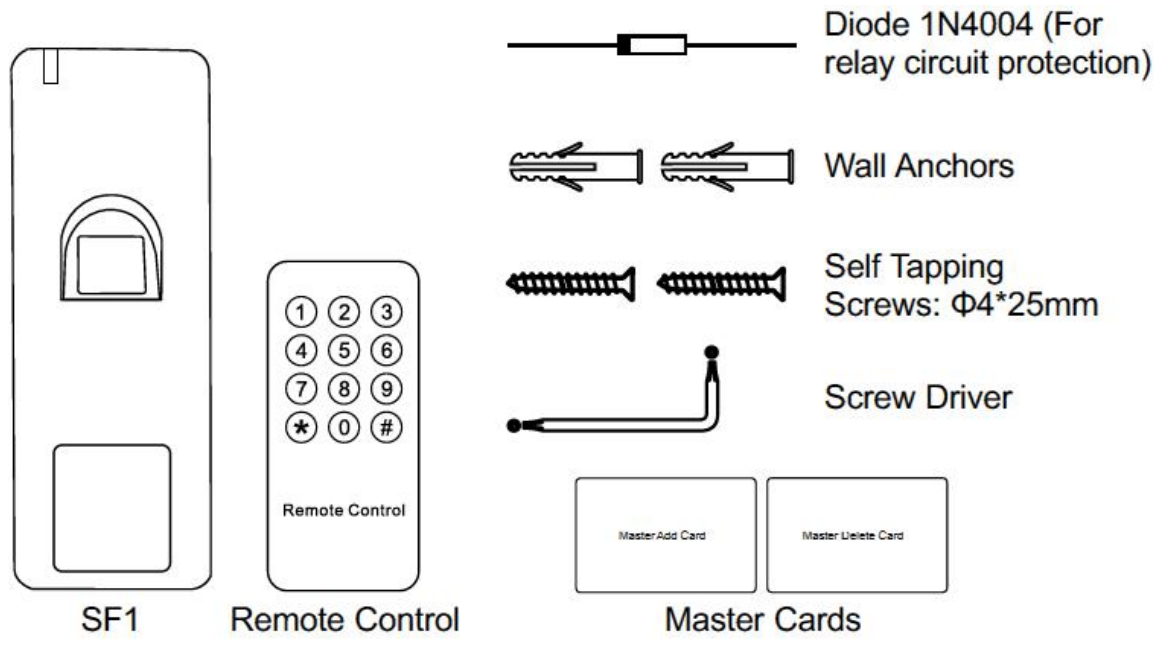


Fig. 2.1. *Lettore BIO CTRL SF1*

Le caratteristiche tecniche del lettore SF1 sono riportate nella Tabella seguente.

☐ Prestazione	Descrizione
Tipo di lettore	Lettore ottico di impronte, risoluzione 500 DPI, tempo di identificazione < 1 s
FAR / FRR	≤ 0,01% / ≤ 0,1%
Ingressi / Uscite	1x ingresso digitale per pulsante di richiesta uscita, 1x per contatto porta 1x uscita di allarme 1x Relè NA-NC-COM, carico max 2A, tempo di commutazione regolabile: 0 ~ 99 s o 0 ~ 3 min; modo bistabile
Interfaccia Wiegand	26 ~ 44 bit (default: 26 bit)
Memoria	1000 impronte e 2000 tessere di prossimità
Alimentazione	12 Vcc ±10%, assorbimento 45 mA (idle), 150 mA max
Dimensioni	48 (L) x 128 (A) x 26 (P) mm
Peso	385 g
Temperatura di utilizzo	-30 °C ~ +60 °C
Umidità di utilizzo	20 ~ 90%
Housing	In lega metallica di zinco con finitura superficiale a polvere; grado di protezione IP66 (uso in esterno)
Portata di lettura	Tag EM 125 kHz: max 2 cm
Modo operativo	Stand-alone o collegamento via Wiegand a host di terze parti

3 Installazione del lettore

Il lettore SF1 deve essere posizionato su una superficie piana ad altezza idonea perché l'utente possa utilizzare la propria impronta digitale per l'identificazione. Far riferimento all'Appendice per ulteriori indicazioni.

In Fig. 3.1 è mostrato schematicamente come eseguire l'installazione del lettore SF1.

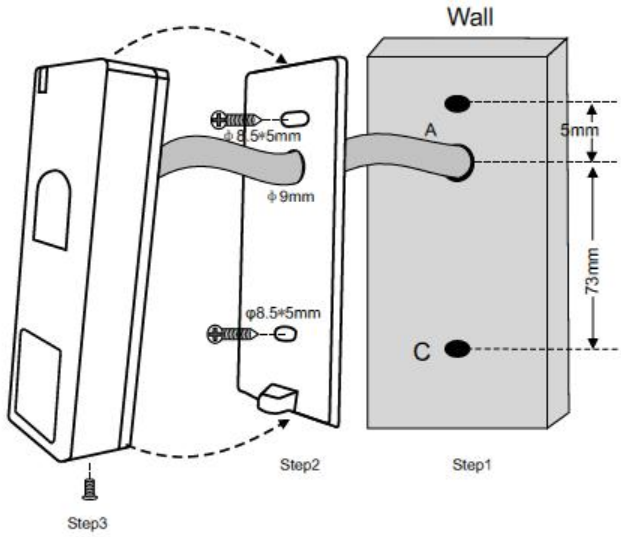


Fig. 3.1. *Montaggio del lettore*

Il significato dei colori dei poli del cavo del lettore è riassunto nella Tabella che segue.

☐ Colore	Funzione	Note
Rosso	12 Vcc	Ingresso 12Vcc da alimentatore
Nero	GND	Ground
Blu	NA relè	Contatto relè NA (usare il diodo fornito)
Porpora	COM relè	Comune del relè
Arancio	NC relè	Contatto relè NC (usare il diodo fornito)
Giallo	OPEN	Ingresso del pulsante di richiesta uscita
Verde	Data 0	Wiegand - D0
Bianco	Data 1	Wiegand - D1
Grigio	Uscita allarme	Contatto negativo per Allarme
Marrone	Contatto porta	Ingresso NC del contatto stato porta

Il significato del LED e del buzzer sono illustrati nella tabella sottostante.

Stato Operativo	LED	Sensore impronte	Buzzer
Stand by	Rosso fisso	Off	--
Ingresso in modo programmazione	Rosso lampeggia	Off	Un beep
In modo programmazione	Arancio fisso	--	Un beep
Errore	--	--	Tre beep
Uscita da modo programmazione	Rosso fisso	--	Un beep
Apertura porta	Verde fisso	Off	Un beep
Allarme	Rosso lampeggia velocemente	Off	Beep continui

Lo schema di connessione del lettore SF1 è illustrato in Fig. 3.2. Notare che l'indicatore 1 è utilizzato per elettroserrature e l'indicatore 2 è utilizzato per elettromagneti. L'uso del diodo di ricircolo 1N4004 fra i poli dell'elettroserratura è fortemente consigliato in entrambi i casi per evitare danni al circuito del relè del lettore.

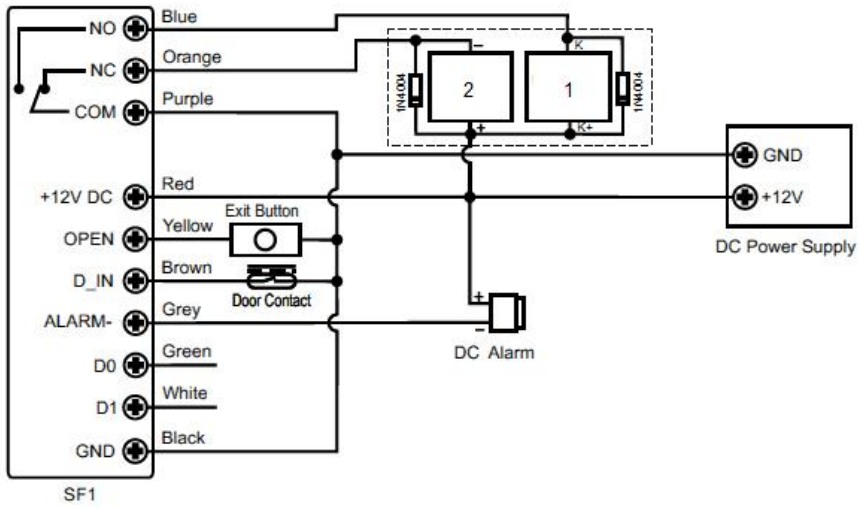


Fig. 3.2. *Schema elettrico dei collegamenti del lettore SF1*

NOTA.

Lo schema elettrico di Fig. 3.2. fa riferimento ad un utilizzo del lettore in modo stand-alone. Qualora sia previsto l'uso con un sistema di controllo accessi di terze parti, utilizzare i collegamenti D0/D1 verso l'host con un doppino twistato (per esempio una coppia di un cavo UTP cat 5E). In collegamento Wiegand con un sistema di controllo accessi, i collegamenti del relè non sono da effettuare: sarà compito della centralina di controllo realizzare la gestione della serratura porta mediante il proprio relè.

4 Programmazione del lettore

4.1 Informazioni generali di programmazione

Nella programmazione delle memorie, il numero ID Utente è un qualsiasi numero fra 1 e 3000. L'ID Utente serve a tenere traccia della posizione di memoria delle diverse impronte così da poter intervenire tutte le volte che sia necessario aggiungere o eliminare impronte digitali in memoria

ATTENZIONE.

La registrazione del numero ID dell'utente è importante: una modifica di credenziali di un utente non può essere fatta se non in possesso dell'ID o di una tessera associata.

Gli ID Utente 997 e 998 sono usati per ID di autorizzazione (utenti che bloccano / sbloccano il lettore).

Gli ID Utente 999 e 1000 sono usati rispettivamente per l'impronta MASTER di aggiunta in memoria e l'impronta MASTER di cancellazione dalla memoria.

Gli ID Utente 2999 e 3000 sono usati rispettivamente per la tessera MASTER di aggiunta in memoria e la tessera MASTER di cancellazione dalla memoria.

Il MASTER può anche essere introdotto via tastierino infrarosso (vd. Fig. 4.1.). In questo caso il codice MASTER è:

123456

Fig. 4.1. *Tastierino infrarosso*

Per modificare il codice MASTER col tastierino infrarosso, seguire i passi seguenti:

- Per entrare in programmazione, digitare sul tastierino: *** (codice MASTER) #**
- Digitare: **0**
- Digitare il nuovo codice: **(nuovo codice MASTER) #**
- Digitare nuovamente il nuovo codice e uscire: **(nuovo codice Master) # ***

Esempio:

- * 123456 #
- 0
- 238046 #
- 238046 # *

Il nuovo codice inserito nell'esempio è 238046 al posto del codice di Default 123456.

ATTENZIONE.

Il codice MASTER deve avere sempre 6 cifre.

Il codice MASTER immesso non deve essere dimenticato o perso. Nel caso effettuare un reset del lettore (vd. Paragrafo 4.10).

Per entrare in programmazione, utilizzare il tastierino infrarosso con la sequenza sopra illustrata: *** (codice MASTER) #**

Le procedure di aggiunta nuovi ID Utente in memoria o di rimozione di ID Utente dalla memoria possono anche essere eseguite dalle tessere di prossimità Master. Nei paragrafi che seguono si fa sempre riferimento al tastierino infrarosso per l'inserimento del codice MASTER.

4.2 Aggiungere impronte in memoria

Se non si desidera sapere in quali locazioni di memoria le impronte saranno memorizzate, per aggiungere nuovi ID Utente con impronta digitale seguire i passi seguenti:

- Entrare in programmazione: *** (codice MASTER) #**
- Digitare: **1**
- Aggiungere la nuova impronta posizionando il dito sul sensore
- Riposizionare nuovamente la nuova impronta sul sensore
- Uscire dalla programmazione: *****

Notare che le impronte digitali per essere memorizzate devono essere posizionate due volte. Dopo l'aggiunta in memoria di una impronta, possono essere memorizzate altre impronte digitali prima di effettuare l'uscita dalla programmazione eseguendo nuovamente i passi 3 e 4 sopra riportati.

Ricordarsi che le impronte saranno memorizzate in locazioni di memoria che il lettore SF1 sceglie autonomamente.

Se la procedura di aggiunta in memoria riguardasse i TAG di prossimità anziché le impronte digitali, invece di presentare l'impronta al sensore due volte, basterebbe avvicinare il TAG 125 kHz al lettore per inserirlo in memoria nelle locazioni da 1001 a 2998 (la scelta della locazione è effettuata autonomamente dal lettore SF1).

In Fig. 4.2 è mostrata la procedura di aggiunta credenziale in memoria usando la tessera MASTER di aggiunta (constrassegnata da **MASTER ADD CARD**).

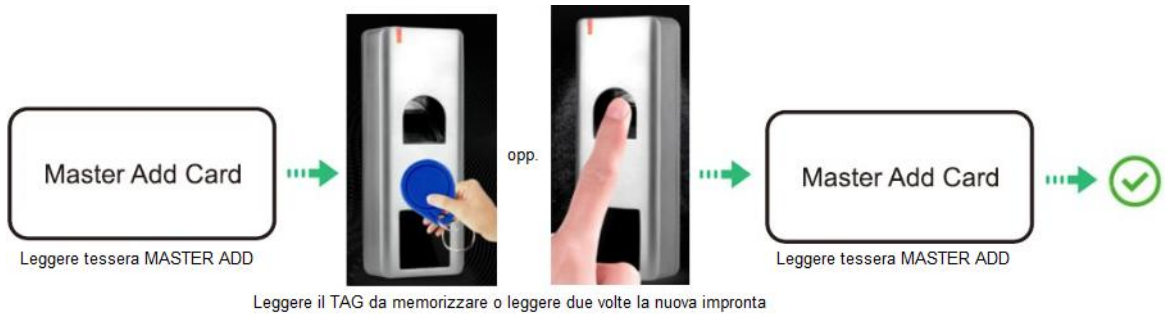


Fig. 4.2. *Aggiunta credenziale in memoria con tessera di prossimità MASTER ADD CARD*

4.3 Aggiungere impronte in locazione di memoria

Se si desidera aggiungere le impronte in una locazione di memoria specifica - così da averne traccia ai fini della successiva eliminazione - seguire i passi seguenti:

- Entrare in programmazione: *** (codice MASTER) #**
- Digitare: **1**
- Digitare la locazione di memoria dove effettuare la memorizzazione: **(User ID) #**
- Aggiungere la nuova impronta posizionando il dito sul sensore
- Riposizionare nuovamente la nuova impronta sul sensore
- Uscire dalla programmazione: *****

Notare che le impronte digitali per essere memorizzate devono essere posizionate due volte e che la procedura di aggiunta in memoria può essere ripetuta per più impronte in successione (vd. Fig. 4.3).

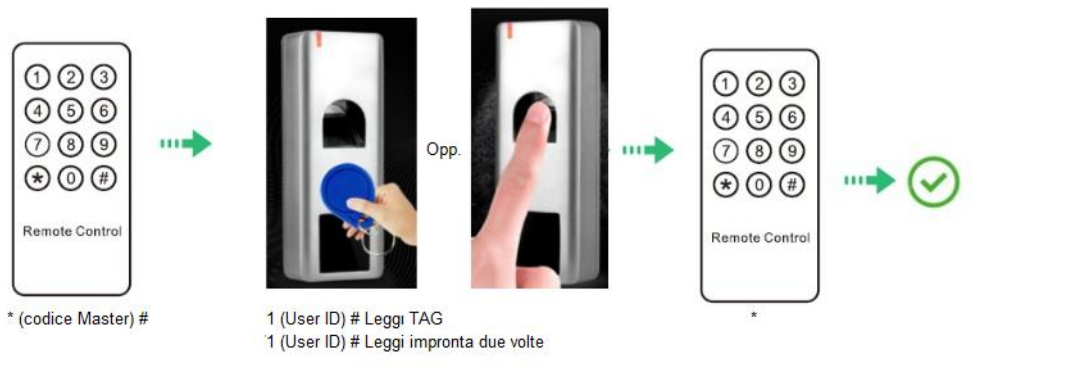


Fig. 4.3. *Aggiunta impronta in memoria in locazione specifica*

NOTA.

Con il termine USER ID si intende la locazione di memoria dove la nuova credenziale verrà memorizzata: quindi è un numero da 1 a 3000. Ricordarsi che le locazioni da 1 a 1000 sono riservate alle impronte digitali e che le locazioni da 1001 a 3000 sono riservate ai TAG di prossimità.

Far anche riferimento alla nota riportata a Pag. 12 circa le locazioni di memoria riservate per funzioni speciali.

4.4 Aggiungere blocchi di TAG in memoria

Per una rapida aggiunta di diversi TAG 125 kHz in memoria, è possibile utilizzare una sequenza che - con una sola operazione di programmazione - aggiunga più di un TAG in memoria purché i codici RFID siano in sequenza numerica.

Seguire i passi seguenti:

- Entrare in programmazione: *** (codice MASTER) #**
- Digitare: **9**
- Digitare la locazione di memoria per la memorizzazione del 1° TAG: **(User ID) #**
- Aggiungere il numero di TAG da aggiungere: **(quantità TAG) #**
- Inserire il codice RFID del 1° TAG: **(da 8 a 10 cifre del 1° TAG) #**
- Uscire dalla programmazione: *****

Notare che i TAG di prossimità spesso riportano scritto in chiaro il proprio codice univoco nella modalità Wiegand: il codice a 26 bit è composto da un bit di start, 24 bit di codice, un bit di stop. I 24 bit di codice, nella forma standard 8,16, sono per esempio mostrati nella tessera di Fig. 4.4.

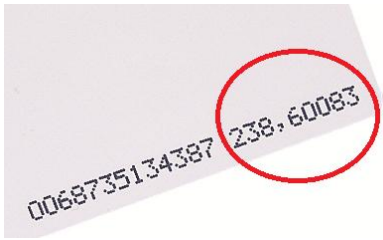


Fig. 4.4. *Codice Wiegand di una tessera 125 kHz*

4.5 Cancellare memorie utente

Per eliminare un singolo utente dalla memoria è necessario utilizzare l'impronta digitale da dover cancellare, oppure il TAG da eliminare o infine sapere la locazione di memoria (User ID) dove la credenziale da eliminare è memorizzata.

Seguire i passi seguenti:

- Entrare in programmazione: *** (codice MASTER) #**
- Digitare: **2**
- Porre sul sensore l'impronta digitare da eliminare - OPPURE
- Presentare al lettore di prossimità il TAG da eliminare - OPPURE
- Digitare la locazione di memoria della credenziale da eliminare: **(User ID) #**
- Uscire dalla programmazione: *****

Prima di uscire dalla procedura di cancellazione, è possibile ripetere i passi 3 o 4 o 5 precedenti per tutte le cancellazioni che si desidera effettuare.

La cancellazione di una credenziale (sia impronta digitale che codice TAG) può avvenire anche attraverso la MASTER DELETE CARD: in questo caso, la sequenza è simile a quella mostrata in Fig. 4.3 dove al posto della MASTER ADD CARD è utilizzata la MASTER DELETE CARD.

Nel caso di cancellazione di una impronta, è sufficiente che l'impronta sia letta una sola volta.

NOTA.

Le impronte memorizzate nelle locazioni di memoria 999 e 1000 sono impronte MASTER per, rispettivamente, aggiunta in memoria e cancellazione della memoria. Queste impronte memorizzabili come descritto nei paragrafi precedenti, si comportano come la tessera MASTER ADD CARD (nel caso dell'impronta il cui User ID è 999) e la tessera MASTER DELETE CARD (nel caso dell'impronta il cui User ID è 1000). Queste impronte non sono quindi utilizzabili per lo sblocco della porta ma solo per l'entrata in modo programmazione.

4.6 Configurare il relè

La configurazione del relè è possibile grazie al menu "3".
Seguire i passi seguenti:

- Entrare in programmazione: *** (codice MASTER) #**
- Digitare: **3**
- Immettere un numero da 1 a 99 per indicare i secondi di impulso del relè: **5 #**
- OPPURE
- Immettere la cifra 0 per indicare che il relè ha un funzionamento bistabile: **0 #**
- Uscire dalla programmazione: *****

Il lettore SF1 è - per default - impostato a modo impulsivo.

4.7 Configurare il modo operativo

La configurazione del modo operativo rappresenta la modalità di funzionamento del lettore: solo TAG, Tag e impronte, solo impronte digitali.
Seguire i passi seguenti:

- Entrare in programmazione: *** (codice MASTER) #**
- Digitare: **4**
- Immettere la cifra 0 per accesso solo con TAG di prossimità: **0 #** - OPPURE
- Immettere la cifra 2 per accesso con Tag o impronte: **2 #** - OPPURE
- Immettere la cifra 3 per accesso con solo impronte digitali: **3 #**
- Uscire dalla programmazione: *****

Il lettore SF1 è - per default - impostato a modo operativo Tag o Impronte.

4.8 Configurare l'allarme

L'allarme può essere attivato (e in tal caso è possibile definire il numero di minuti di allarme attivo) o disattivato. Per attivarlo, seguire i passi seguenti:

- Entrare in programmazione: *** (codice MASTER) #**
- Digitare: **5**
- Immettere la cifra 0 per disattivare l'allarme: **0 #** - OPPURE

- Immettere 1, 2 o 3 per determinare il numero di minuti in cui l'allarme rimarrà attivo: **1 #**
- Uscire dalla programmazione: *****

Il lettore SF1 ha - per default - un allarme impostato a 1 minuto.

Notare che l'allarme si attiva in una delle modalità esposte nei seguenti sotto-paragrafi.

4.8.1 Allarme strike-out

L'allarme strike out si attiva quando, per 10 volte consecutive, si ha un tentativo di accesso non autorizzato, per esempio dopo 10 impronte o tessere che non sono riconosciute dal lettore. L'allarme strike-out, quando attivo, nega la possibilità di effettuare qualsiasi accesso.

Seguire i passi seguenti:

- Entrare in programmazione: *** (codice MASTER) #**
- Digitare: **5**
- Immettere la cifra 4 per disattivare l'allarme strike-out: **4 #** - OPPURE
- Immettere la cifra 5 per negare l'accesso per 10 minuti: **5 #** - OPPURE
- Immettere la cifra 6 perché solo un TAG o una impronta validi possano annullare l'allarme di strike-out: **6 #**
- Uscire dalla programmazione: *****

Il lettore SF1 ha - per default - l'allarme di strike-out disabilitato.

4.8.2 Allarme porta

L'allarme porta si attiva in due casi: se la porta viene aperta senza che sia stato presentato alcuna tessera o impronta valida (porta forzata) oppure quando, in presenza di credenziale valida, la porta rimane aperta troppo a lungo (il tempo di porta aperta troppo a lungo è fissato in un minuto e non può essere modificato).

Affinché l'allarme porta possa essere rilevato, è quindi necessario che il contatto magnetico di porta sia cablato al lettore SF1.

Nel caso di porta aperta troppo a lungo, il buzzer interno del lettore inizierà a ronzare automaticamente dopo il minuto di timeout: il buzzer si arresta quando la porta viene chiusa o un utente valido o il master si identificano: viceversa il lettore continuerà a ronzare per tutto il tempo definito dalla funzione allarme porta (vd. 4.8).

Nel caso di porta forzata, il buzzer interno e l'output di allarme vengono attivati immediatamente al momento dell'apertura porta e possono essere arrestati solo dall'identificazione di un utente valido o del master: viceversa il lettore continuerà a ronzare per tutto il tempo definito dalla funzione allarme porta (vd. 4.8).

Per configurare la rilevazione dello stato porta, seguire i passi seguenti:

- Entrare in programmazione: *** (codice MASTER) #**
- Digitare: **6**
- Immettere la cifra 0 per disattivare l'allarme porta: **0 #** - OPPURE
- Immettere la cifra 1 per attivare l'allarme porta: **1 #**
- Uscire dalla programmazione: *****

Il lettore SF1 ha - per default - l'allarme porta disabilitato.

4.9 Uso del lettore per l'accesso stand-alone

Per ottenere l'accesso - cioè l'attivazione del relè per lo sblocco della serratura porta - posizionare un'impronta valida sul sensore impronte o presentare un TAG di prossimità valido - memorizzati nel lettore come descritto ai paragrafi 4.2 e 4.3.

Il relè rimarrà eccitato per tutto il tempo programmato (vd. Paragrafo 4.6).

4.10 Reset delle tessere MASTER

Se, per qualsiasi motivo, si fossero perse le tessere MASTER ADD CARD e MASTER DELETE CARD, queste possono essere ricreate effettuando una procedura di ripristino.

ATTENZIONE.

Il ripristino descritto in questo paragrafo comporta solo l'annullamento delle tessere MASTER: tutte le memorie utente (User ID) e i valori di tutti gli altri parametri rimangono immutati.

La procedura per il reset è la seguente:

- Spegnere il lettore, togliendo l'alimentazione
- Premere e tener premuto il pulsante di richiesta di uscita (qualora il pulsante non fosse presente, effettuare un corto-circuito fra i poli GIALLO e NERO)
- Ridare alimentazione al lettore: saranno emessi due beep
- Rilasciare il pulsante di apertura porta (o scollegare il ponticello fra i poli GIALLO e NERO)
- Il LED si accenderà in colore arancione
- Leggere in successione due TAG o tessere (in tecnologia EM 125 kHz) entro 10 secondi: la prima tessera diventerà la nuova MASTER ADD CARD e la seconda tessera diventerà la nuova MASTER DELETE CARD
- Il LED commuterà a rosso per indicare che il reset è concluso.

Notare che le nuove tessere MASTER possono essere qualsiasi tessera o TAG di tecnologia EM 125 kHz. I due TAG devono essere diversi.

4.11 Uso del lettore come slave Wiegand

Quando si vuole che il lettore SF1 sia utilizzato come "slave" di un impianto di controllo accessi con un collegamento Wiegand, le credenziali vengono trasmesse sul bus D0/D1 secondo le modalità seguenti.

4.11.1 Codice sito del lettore

Nel codice Wiegand 26, i primi 8 bit dopo il bit di start rappresentano il codice sito di un impianto. Per configurare il codice sito, seguire i passi seguenti:

- Entrare in programmazione: *** (codice MASTER) #**
- Digitare: **7**

- Immettere il codice sito come numero compreso fra 0 e 255: es. **82 #**
- Uscire dalla programmazione: *****

Il lettore SF1 ha - per default - il codice sito a 0.

Nell'esempio sopra riportato (codice sito 82), quando un utente si identifica sul lettore con la propria impronta digitale, memorizzata in una delle locazioni di memoria (supponiamo la 566), allora il codice Wiegand che il lettore trasmette all'host per l'autorizzazione all'accesso è: **082,00566** codice che viene chiamato tessera RFID virtuale.

Un codice di questo tipo potrebbe essere identico a quello scritto su una tessera RFID (si veda l'esempio di Fig. 4.4).

NOTA.

Questo tipo di invio codici Wiegand si applica alle sole impronte digitali.

4.11.2 Impostazione formato Wiegand del lettore

Il lettore SF1 utilizza lo standard Wiegand da 26 bit fino a 44 bit. Per impostare il tipo di output utilizzare i passi seguenti:

- Entrare in programmazione: *** (codice MASTER) #**
- Digitare: **8**
- Immettere il tipo di standard Wiegand con un numero da 26 a 44: **26 #** - OPPURE
- Disabilitare l'output Wiegand: **0 #**
- Uscire dalla programmazione: *****

Il lettore SF1 ha - per default - lo stadard Wiegand 26 bit.

4.12 Blocco del lettore

Il lettore SF1 può essere bloccato da un utente autorizzato: questo è il caso in cui un amministratore rende possibile agli altri utenti di eseguire l'accessso solo dopo essersi identificato.

Per questo tipo di funzione sono state riservate due locazioni di memoria speciali: la 997 e la 998.

Qualora siano state programmate delle impronte digitali nelle locazioni di memoria 997 e 998, il lettore può essere bloccato come da procedura seguente:

- Il lettore si trova in modalità operativa normale (stand-by)
- L'utente la cui impronta è memorizzata in locazione 997 si identifica sul lettore
- Il LED rosso lampeggia 4 volte
- Tutti gli utenti, anche se in possesso di credenziale valida, non sono più in grado di effettuare l'accesso: se provassero a identificarsi con la propria impronta otterrebbero solo 3 beep brevi dal buzzer. Il pulsante di apertura porta consente sempre l'attivazione del relè.
- Quando l'utente 997 si identifica nuovamente sul lettore di impronte, si ottiene lo sblocco segnalato da 4 lampeggi del LED verde: il lettore ritorna alla normale operatività.

L'impronta della locazione di memoria 998 si comporta al medesimo modo e può essere una seconda impronta dello stesso amministratore o un'impronta digitale di un diverso utente.

4.13 Manutenzione

Il lettore SF1 non presenta specifiche necessità di manutenzione. Si raccomandano i seguenti punti:

- Utilizzare sempre un alimentatore che corrsiponda ai valori di tensione e assorbimento dichiarati dal produttore.
- Pulire con regolarità il vetro a protezione del sensore ottico, evitando di graffiarlo. Non usare agenti chimici aggressivi ma solo acqua possibilmente distillata. Per la pulizia del sensore utilizzare sempre un panno morbido evitando che la superficie di lettura venga graffiata o segnata. Non utilizzare per nessun motivo detergenti quali benzene, alcool o detersivi chimici per non danneggiare la superficie di lettura.
- Non disassemblare mai il lettore. Se per qualsiasi motivo emergesse un problema con il dispositivo, si prega di restituirlo per riparazione o sostituzione (a insindacabile giudizio del produttore).

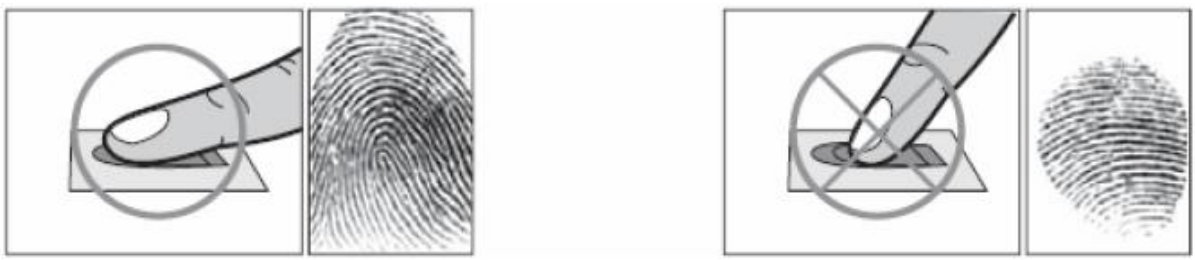
5 Appendice

5.1 Posizionamento del dito sul sensore ottico

Nell'uso del lettore, far riferimento ai suggerimenti seguenti.

- Cercare sempre di coprire totalmente la superficie del sensore
- Porre l'impronta il più possibile al centro del sensore. Normalmente si tende a porre la parte superiore dell'impronta sul sensore: la parte più rilevante dell'impronta si trova al centro del polpastrello, circa nel punto opposto a dove l'unghia emerge dalla pelle superiore del dito. La base dell'unghia dovrebbe trovarsi quindi al centro della superficie di lettura.
- Se il dito viene posizionato sul sensore in modo non corretto, solo una frazione dell'impronta viene letta pregiudicando il processo di lettura.

La figura qui sotto mostra a sinistra come posizionare correttamente l'impronta sul sensore.



Il lettore è stato progettato e sviluppato per identificare impronte digitali indipendentemente dalla condizione della pelle. Se il lettore non riuscisse a leggere l'impronta, provare con i suggerimenti seguenti:

- Se il dito fosse bagnato o sudato, asciugarlo prima di un qualsiasi lettura
- Assicurarsi che sia il dito che la superficie del sensore siano pulite
- Se la condizione del polpastrello fosse di estrema secchezza, alitare brevemente sul dito.
- Se una impronta viene letta raramente, eliminarla ed effettuare un ulteriore apprendimento.
- Se – per motivi funzionali – un polpastrello avesse tagli permanenti e/o problemi di acquisizione, tentare con un differente dito, se necessario dell'altra mano.

NOTA.

Nel caso un'impronta non venga letta, controllare per prima cosa i diritti di accesso per quell'utente - sia nella memoria del lettore che nel sistema di controllo accesso (qualora il lettore sia utilizzato come slave).