



Ⓟ Instrukcja obsługi

System kontroli dostępu – WLAN/ RFID/ odcisk palca

Nr zamówienia 3060831



1 Spis treści



2	Wprowadzenie	5
3	Dokumentacja produktu	5
4	Użytkowanie zgodne z przeznaczeniem.....	5
5	Zakres dostawy.....	6
6	Objaśnienia symboli.....	6
7	Wskazówki dotyczące bezpieczeństwa	7
8	Elementy obsługi i złącza	8
9	Montaż i podłączenie	9
	9.1 Montaż	9
	9.2 Podłączanie do standardowego źródła zasilania.....	10
	9.3 Podłączanie do instalacji alarmowej.....	11
	9.4 Złącze Wiegand	12
	9.4.1 Korzystanie z systemu kontroli dostępu jako czytnika zewnętrznego	12
	9.4.2 Podłączanie zewnętrznego czytnika do systemu kontroli dostępu.....	13
	9.5 Podłączanie dwóch systemów kontroli dostępu dla trybu blokady.....	14
10	Konfigurowanie	15
11	Uruchamianie.....	15
12	Programowanie.....	16
	12.1 Dobra praktyka	16
	12.2 Ogólne informacje.....	16
	12.3 Resetowanie wszystkich ustawień do ustawień fabrycznych; programowanie transpondera głównego... 17	
	12.3.1 Resetowanie systemu kontroli dostępu i programowanie transpondera głównego.....	17
	12.3.2 Resetowanie systemu kontroli dostępu bez programowania transpondera głównego.....	17
	12.3.3 Przegląd ustawień standardowych.....	18
	12.4 Aktywacja/dezaktywacja trybu programowania	18
	12.5 Zmiana kodu głównego.....	19
	12.6 Programowanie/usuwanie głównego odcisku palca	19
	12.6.1 Programowanie głównego odcisku palca	19
	12.7 Usuwanie głównego odcisku palca.....	20
	12.8 Ustawianie trybu pracy dla złącza Wiegand	20
	12.9 Konfigurowanie rozpoznawania otwarcia drzwi	21
	12.10 Aktywacja/dezaktywacja trybu blokady.....	22
	12.11 Wybór trybu dostępu	23
	12.12 Zapisywanie PINu użytkownika	24
	12.12.1 Automatyczne zapisanie PINu użytkownika w następnym wolnym miejscu w pamięci.....	24

12.12.2	Przypisanie PINu użytkownika do określonego miejsca w pamięci	25
12.13	Usuwanie PINu użytkownika	26
12.13.1	Usuwanie PINu użytkownika.....	26
12.13.2	Usuwanie PINu użytkownika za pomocą numeru miejsca w pamięci.....	26
12.14	Programowanie transpondera użytkownika.....	27
12.14.1	Automatyczne zapisanie transpondera użytkownika w kolejnym wolnym miejscu w pamięci	27
12.14.2	Przypisanie transpondera użytkownika do określonego miejsca w pamięci.....	28
12.14.3	Programowanie kilku transponderów użytkownika z kolejnym numerem transpondera.....	28
12.14.4	Programowanie transponderów użytkowników w trybie zbiorczym	29
12.15	Usuwanie transpondera użytkownika	30
12.15.1	Usuwanie transpondera użytkownika za pomocą transpondera	30
12.15.2	Usuwanie transpondera użytkownika za pomocą numeru transpondera	30
12.15.3	Usuwanie transpondera użytkownika za pomocą numeru miejsca w pamięci	31
12.16	Programowanie odcisku palca użytkownika	31
12.16.1	Automatyczne zapisanie odcisku palca użytkownika w następnym wolnym miejscu w pamięci	31
12.16.2	Przypisywanie odcisku palca użytkownika do określonego miejsca w pamięci.....	32
12.17	Usuwanie odcisku palca użytkownika.....	33
12.17.1	Usunięcie odcisku palca użytkownika za pomocą odcisku palca	33
12.17.2	Usuwanie odcisku palca użytkownika za pomocą numeru miejsca w pamięci.....	33
12.18	Usuwanie wszystkich miejsc w pamięci.....	34
12.19	Ustawianie czasu aktywacji dla styku przełącznego.....	34
12.20	Aktywacja lub dezaktywacja zabezpieczenia przed błędnymi wpisami	35
12.21	Ustawianie czasu trwania alarmu dla funkcji zabezpieczenia	35
12.22	Aktywacja dostępu dla gości.....	35
12.22.1	Programowanie transpondera gościa	36
12.22.2	Zapisywanie PINu gościa.....	37
12.22.3	Usuwanie transpondera gościa lub PINu gościa	37
12.23	Dodawanie użytkowników antynapadowych.....	38
12.24	Aktywacja/dezaktywacja wskazania optycznego i akustycznego	39
12.25	Aktywacja sieci WLAN	39
12.26	Transmisja danych pomiędzy dwoma systemami kontroli dostępu	40
12.27	Ustawianie formatu wejściowego danych Wiegand.....	41
12.28	Ustawianie formatu wyjściowego danych Wiegand	42
13	Obsługa	43
13.1	Dostęp za pomocą ważnego PINu/ transpondera/ odcisku palca użytkownika.....	43
13.2	Dostęp poprzez przycisk automatu do otwierania drzwi.....	43
13.3	Zapobieganie odczytaniu PINu.....	43

13.4 Dezaktywacja alarmu/blokady w przypadku nieprawidłowego wpisu	43
14 Rozwiązywanie problemów	44
15 Deklaracja zgodności (DOC)	46
16 Konserwacja i czyszczenie	46
17 Utylizacja	46
18 Dane techniczne	47
18.1 Oprogramowanie	47
18.2 Zasilanie	47
18.3 Dostęp	47
18.4 Wyjście	47
18.5 Otoczenie	47
18.6 Inne	47

2 Wprowadzenie

Dziękujemy za zakup naszego produktu.

Produkt ten spełnia krajowe i europejskie wymogi prawne. Aby utrzymać ten stan i zapewnić bezpieczną eksploatację, użytkownik musi przestrzegać niniejszej instrukcji obsługi!



Niniejsza instrukcja obsługi jest częścią tego produktu. Zawiera ona ważne wskazówki dotyczące uruchamiania i użytkowania produktu. Należy o tym pamiętać, gdy produkt przekazywany jest osobom trzecim. Zachowaj niniejszą instrukcję obsługi do wykorzystania w przyszłości!

Wszystkie zawarte w instrukcji obsługi nazwy firm i produktów są znakami towarowymi należącymi do ich właścicieli. Wszelkie prawa zastrzeżone.

Potrzebujesz pomocy technicznej? Skontaktuj się z nami:

E-mail: bok@conrad.pl

Strona www: www.conrad.pl

Dane kontaktowe znajdują się na stronie kontakt: <https://www.conrad.pl/kontakt>

Dystrybucja Conrad Electronic Sp. z o.o. ul. Książnica 12, 31-637 Kraków, Polska

3 Dokumentacja produktu

Produkt jest udokumentowany różnymi instrukcjami:

- Wskazówki dotyczące bezpieczeństwa
- Instrukcja programowania
- Instrukcja instalacji i obsługi sprzętu (do pobrania)
- Instrukcja konfiguracji i obsługi aplikacji mobilnej (do pobrania)



Skorzystaj z linku www.conrad.com/downloads (lub zeskanuj kod QR), aby pobrać instrukcję obsługi (lub nowe/aktualne wersje, jeśli są dostępne). Postępuj zgodnie z instrukcjami na stronie internetowej.

4 Użytkowanie zgodne z przeznaczeniem

Produkt służy głównie do zabezpieczania dostępu do drzwi (np. biura) lub aktywacji/dezaktywacji instalacji alarmowej. Produktem można sterować przy użyciu następujących metod uwierzytelniania:

- Klawiatura (uwierzytelnianie kodem PIN)
- Transponder (uwierzytelnianie za pomocą karty Smartcard)
- Odcisk palca
- Aplikacja mobilna (Tuya Smart Life - Smart Living) (uwierzytelnianie kodem PIN i uwierzytelnianie zdalne)

Można zapisać maksymalnie 900 kodów PIN/transponderów i 100 odcisków palców dla różnych typów użytkowników. Jeśli uwierzytelnienie użytkownika powiedzie się, aktywowany zostanie bezpotencjałowy styku przełączny przekaźnika.

Produkt jest przeznaczony do montażu na ścianie i może pracować wewnątrz i na zewnątrz (IP66).

Ze względów bezpieczeństwa oraz certyfikacji produktu nie można w żaden sposób przebudowywać i/lub modyfikować. W przypadku korzystania z produktu w celach innych niż opisane może on ulec uszkodzeniu. Nieprawidłowe użytkowanie produktu może również prowadzić do zagrożeń, takich jak zwarcia, pożary lub porażenia prądem.

Należy uważnie przeczytać instrukcję obsługi i przechowywać ją w bezpiecznym miejscu. Produkt można przekazywać osobom trzecim wyłącznie z załączoną instrukcją obsługi.

Produkt jest zgodny z wymogami prawnymi i spełnia wszystkie przepisy krajowe i europejskie. Wszystkie zawarte w instrukcji obsługi nazwy firm i produktów są znakami towarowymi należącymi do ich właścicieli. Wszelkie prawa zastrzeżone.

5 Zakres dostawy

- System kontroli dostępu (z kablem o długości 90 cm)
- Karta główna (Master)
- Klucz L
- 2 x śruba
- 2 x kolek rozporowy
- Dioda 1N4004 (do styku przełącznego przekaźnika)
- Dokumentacja produktu

6 Objaśnienia symboli

W tekście występują następujące symbole:



Symbol białej błyskawicy w trójkącie jest stosowany, gdy istnieje ryzyko dla zdrowia, np. na skutek porażenia prądem.



Symbol z wykrzyknikiem w trójkącie wskazuje na ważne informacje w tej instrukcji obsługi. Zawsze dokładnie czytaj te informacje.



Symbol ze strzałką można znaleźć tam, gdzie odpowiednio oznaczony rozdział zawiera specjalne wskazówki i informacje dotyczące obsługi.

7 Wskazówki dotyczące bezpieczeństwa



Uszkodzenia spowodowane nieprzestrzeganiem niniejszych wskazówek dotyczących bezpieczeństwa obsługi powodują unieważnienie rękojmi/gwarancji! Nie ponosimy odpowiedzialności za szkody następujące!

Nie ponosimy odpowiedzialności za obrażenia oraz straty materialne spowodowane nieprawidłową obsługą lub nieprzestrzeganiem wskazówek bezpieczeństwa! W takich przypadkach wygasa rękojmia/gwarancja.

- Produkt nie jest zabawką. Przechowuj go w miejscu niedostępnym dla dzieci i zwierząt.
- Należy chronić produkt przed ekstremalnymi temperaturami, silnymi wibracjami, palnymi gazami, oparami i rozpuszczalnikami. System kontroli dostępu nadaje się do montażu i użytkowania wewnątrz pomieszczeń oraz w strefie zewnętrznej (IP66).
- Z produktem należy obchodzić się ostrożnie. Wstrząsy, uderzenia lub upadek produktu nawet z niewielkiej wysokości spowodują jego uszkodzenie. Nie narażać produktu na obciążenia mechaniczne.
- Montaż i podłączenie dozwolone są tylko po odłączeniu napięcia.
- Nie należy nigdy przekraczać obciążalności styku przełącznego podanej w rozdziale „Dane techniczne”.



Ostrożnie!

Nigdy nie należy przełączać napięcia sieciowego. Istnieje wówczas zagrożenie dla życia przez porażeniem prądem elektrycznym!

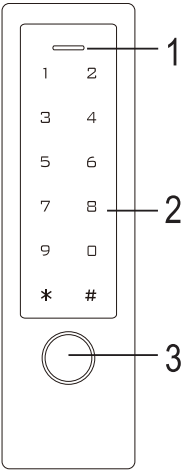
- Przestrzegać wskazówek dot. bezpieczeństwa i instrukcji obsługi innych urządzeń, do których jest podłączony niniejszy produkt (np. automat do otwierania drzwi, instalacja alarmowa).
- Jeśli bezpieczna praca nie jest już możliwa, należy przerwać użytkowanie i zabezpieczyć produkt przed niezamierzonym użyciem. Nie można zagwarantować bezpiecznej pracy, jeżeli produkt wykazuje widoczne uszkodzenia, nie działa prawidłowo, był przechowywany przez dłuższy czas w niekorzystnych warunkach otoczenia lub został poddany znacznym obciążeniom transportowym.
- W zakładach prowadzących działalność gospodarczą należy przestrzegać przepisów o zapobieganiu nieszczęśliwym wypadkom stowarzyszenia branżowego, dotyczących urządzeń elektrycznych i środków technicznych.
- Nie pozostawiać opakowań bez nadzoru. Mogą one stać się niebezpieczną zabawką dla dzieci!
- Prace konserwacyjne, regulacyjne i naprawy może przeprowadzać wyłącznie specjalista lub specjalistyczny warsztat.
- Jeśli nie ma się pewności co do prawidłowego użytkowania lub jeśli pojawiają się pytania, na które odpowiedzi nie można znaleźć w tej instrukcji obsługi, prosimy o kontakt z nami lub z innym specjalistą.

8 Elementy obsługi i złącza

- 1 Wskaźnik pracy LED
- 2 Klawiatura z wbudowanym za nią czujnikiem RFID
- 3 Czujnik linii papilarnych z pierścieniem LED

Kabel przyłączeniowy:

Kolor	Napis	Funkcja
Czerwony	DC +	Zasilanie 12–18 V/DC
Czarny	GND	GND/masa
Niebieski	Relay NO (przełącznik NO)	Zestyk NO (zestyk zwierny) przełącznika
Fioletowy	Relay common (przełącznik wspólny)	Wspólne przyłącze dla wyjścia przełącznika
Pomarańczowy	Relay NC (przełącznik NC)	Standardowo zamknięte wyjście przełącznika (zainstaluj diodę wchodzącą w zakres dostawy)
Brązowy	Wejście zestyku	Wejście zestyku drzwi/bramy (standardowo zamknięte)
Szary	Wyjście alarmowe	Zestyk NC (standardowo zamknięty) przełącznika
Żółty	OPEN	Wejście dla żądania wyjścia (REX)
Biały	D1	Dane Wiegand 1
Zielony	D0	Dane Wiegand 0



➔ Jeśli system kontroli dostępu jest podłączony do sterownika Wiegand jako czytnik zewnętrzny, żółty przewód systemu kontroli dostępu może (w razie potrzeby) służyć jako sterowanie sygnału dźwiękowego (niski poziom = dźwięk aktywowany) zamiast sygnalizacji automatu do otwierania drzwi.

9 Montaż i podłączenie



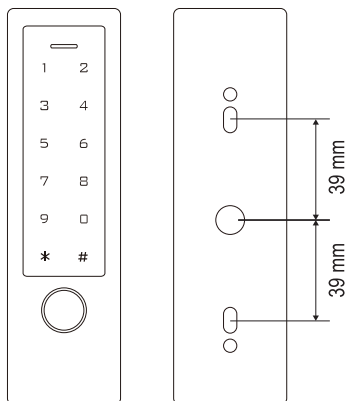
Upewnić się, że kable połączeniowe nie są zagięte ani zgniecione. Może to prowadzić do nieprawidłowego działania, zwarcia i uszkodzenia urządzenia. Podczas wiercenia i dokręcania śrub należy uważać, aby nie uszkodzić żadnych kabli ani przewodów. Montaż i podłączanie dozwolone są wyłącznie po odłączeniu napięcia.

9.1 Montaż



Ostrożnie!

Przez bezpotencjałowy styk przełączny nie można nigdy prowadzić napięcia sieciowego! Istnieje zagrożenie życia wskutek porażenia prądem elektrycznym! Zwróć uwagę na dopuszczalną obciążalność styku (moc załączalną), patrz rozdział „Dane techniczne”.



- Wykręć śrubę znajdującą się w dolnej części systemu kontroli dostępu.
- Podnieś system kontroli dostępu z płyty montażowej i zdejmij panel przedni.
- Zamontuj płytę montażową w miejscu montażu za pomocą odpowiednich śrub i kołków.
- Zamocuj system kontroli dostępu na płycie montażowej i zabezpiecz go ponownie śrubą.

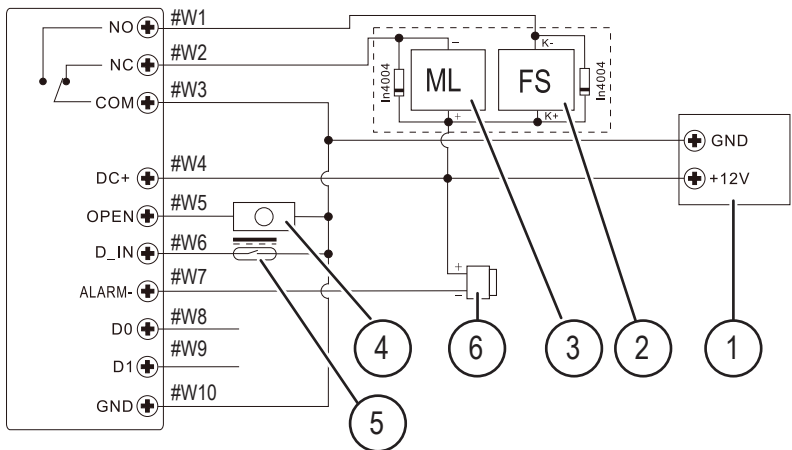
9.2 Podłączanie do standardowego źródła zasilania

Podłącz system kontroli dostępu do standardowego źródła zasilania i wybierz odpowiednią opcję:

- **Automat do otwierania drzwi „Fail-Secure”**: Automat do otwierania drzwi zwalnia rygiel blokujący tylko po przyłożeniu napięcia roboczego (zwykła wersja dla drzwi domowych).
- **Automat do otwierania drzwi „Fail-Safe”**: Automat do otwierania drzwi zwalnia rygiel blokujący tylko w przypadku braku napięcia roboczego (dość rzadka konstrukcja, np. w przypadku drzwi drogi ewakuacyjnej, które można otworzyć w przypadku awarii zasilania).

Automat do otwierania drzwi „Fail-Secure”

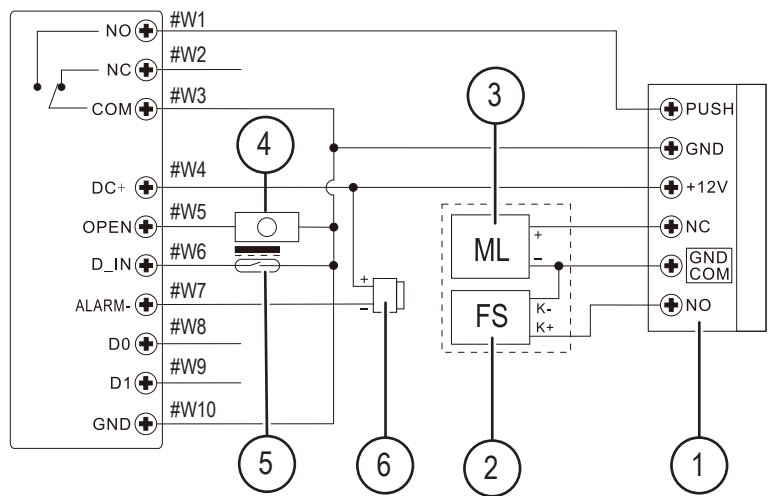
➔ Zalączona dioda musi być podłączona poprawnie w pobliżu automatu do otwierania drzwi, aby chronić system kontroli dostępu przed skokami napięcia. Należy przestrzegać kierunku podłączania.



	Elementy		Elementy
1	Zasilanie	4	Przycisk EXIT
2	Zamek Fail-Secure	5	Zestyk drzwiowy
3	Zamek magnetyczny lub zamek Fail Safe	6	Alarm

	Kolor przewodu		Kolor przewodu
#W1	Niebieski	#W6	Brązowy
#W2	Pomarańczowy	#W7	Szary
#W3	Fioletowy	#W8	Zielony
#W4	Czerwony	#W9	Biały
#W5	Żółty	#W10	Czarny

Automat do otwierania drzwi „Fail-Safe”



	Elementy		Elementy
1	Zasilanie	4	Przycisk EXIT
2	Zamek Fail-Secure	5	Zestyk drzwiowy
3	Zamek magnetyczny lub zamek Fail Safe		

	Kolor przewodu		Kolor przewodu
#W1	Niebieski	#W6	Brązowy
#W2	Pomarańczowy	#W7	Szary
#W3	Fioletowy	#W8	Zielony
#W4	Czerwony	#W9	Biały
#W5	Żółty	#W10	Czarny

9.3 Podłączanie do instalacji alarmowej

Należy postępować zgodnie z instrukcją obsługi stosowanej instalacji alarmowej. Przekaznik w systemie kontroli dostępu przełącza się po rozpoznaniu ważnego kodu użytkownika lub transpondera albo po dotknięciu czujnika palcem, którego odcisk jest zapisany w pamięci. W ten sposób instalację alarmową można uzbroić lub rozbroić.

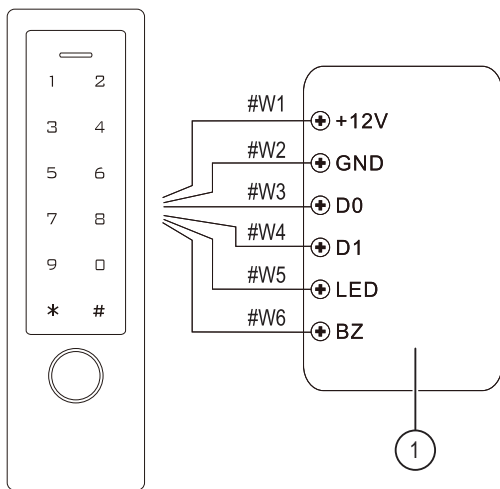
9.4 Złącze Wiegand

Złącze Wiegand systemu kontroli dostępu można wykorzystać na dwa różne sposoby.

9.4.1 Korzystanie z systemu kontroli dostępu jako czytnika zewnętrznego

System kontroli dostępu można podłączyć do odpowiedniego sterownika Wiegand, gdzie służy jako czytnik zewnętrzny. W tym trybie pracy nie działają prawie wszystkie ustawienia systemu kontroli dostępu.

- Żółty przewód systemu kontroli dostępu nie służy poza tym już jako sygnalizacja automatu do otwierania drzwi, lecz (w razie potrzeby) jako sterowanie sygnałem dźwiękowym (niski poziom = dźwięk aktywowany).
- System kontroli dostępu pracuje z napięciem roboczym 12–18 V/DC. Jeśli sterownik Wiegand nie zapewnia takiego napięcia, do systemu kontroli dostępu potrzebny będzie oddzielny zasilacz. Okablowanie należy wtedy wykonać inaczej niż na rysunku.
- W systemie kontroli dostępu można zaprogramować szybkość transmisji danych, która musi być identyczna z szybkością sterownika Wiegand. Należy przestrzegać instrukcji obsługi sterownika Wiegand.



	Elementy
1	Sterowanie dostępem

	Kolor przewodu		Kolor przewodu
#W1	Czerwony	#W4	Biały
#W2	Czarny	#W5	Brązowy
#W3	Zielony	#W6	Żółty

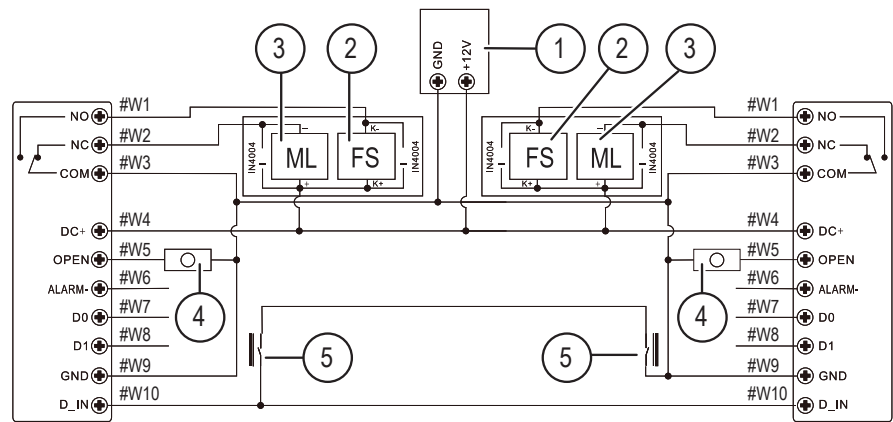
9.4.2 Podłączanie zewnętrznego czytnika do systemu kontroli dostępu

Sam system kontroli dostępu pracuje jako sterownik Wiegand i umożliwia obsługę czytnika zewnętrznego (np. do transpondera).

- Obsługiwane są czytniki kart do transponderów 125 kHz.
- Transpondery można programować zarówno za pośrednictwem systemu kontroli dostępu, jak i czytnika kart (w razie problemów do programowania należy używać wyłącznie zewnętrznych czytników kart).
- Zwróć uwagę na to, aby nie zamienić obu przewodów danych D0 i D1; D0 musi być zawsze podłączone do D0, a D1 do D1. W każdym przypadku należy postępować zgodnie z instrukcją obsługi stosowanego zewnętrznego czytnika kart.
- W systemie kontroli dostępu można zaprogramować szybkość transmisji danych, która musi być identyczna z szybkością czytnika. Należy przestrzegać instrukcji obsługi czytnika.

9.5 Podłączanie dwóch systemów kontroli dostępu dla trybu blokady

Dla trybu blokady skonfiguruj dwa systemy kontroli dostępu i dwoje drzwi. Dwa systemy kontroli dostępu zapewniają, że tylko jedno drzwi mogą być otwarte w danym momencie: Jeśli jedno drzwi są otwarte, drugie muszą być zamknięte.



	Elementy		Elementy
1	Zasilanie	4	Przycisk EXIT
2	Zamek Fail-Secure	5	Zestyk drzwiowy
3	Zamek magnetyczny lub zamek Fail Safe		

	Kolor przewodu		Kolor przewodu
#W1	Niebieski	#W6	Szary
#W2	Pomarańczowy	#W7	Zielony
#W3	Fioletowy	#W8	Biały
#W4	Czerwony	#W9	Czarny
#W5	Żółty	#W10	Brązowy

- Podłącz funkcję blokady zgodnie ze schematem połączeń blokady.
- Przed użyciem trybu blokady należy go skonfigurować na obu urządzeniach. Dalsze informacje na ten temat można znaleźć w rozdziale [„12.10 Aktywacja/dezaktywacja trybu blokady” na stronie 22.](#)

10 Konfigurowanie

Po zakończeniu montażu i podłączeniu włącz napięcie robocze. System kontroli dostępu wyemituje krótki sygnał dźwiękowy i nastąpi aktywacja podświetlenia przycisków. Dioda LED świeci się na czerwono – oznacza to, że system kontroli dostępu znajduje się w trybie gotowości (standby).

System kontroli dostępu wyłącza automatycznie podświetlenie przycisków po 20 sekundach, jeśli nie wykryje dotknięcia pola czujnika.

System kontroli dostępu jest gotowy do programowania.

11 Uruchamianie

Po podłączeniu i zamontowaniu systemu kontroli dostępu należy go włączyć. Po włączeniu system kontroli dostępu wyemituje sygnał dźwiękowy, a dioda LED będzie się świecić stale na czerwono (tryb gotowości).

System kontroli dostępu jest teraz gotowy do pracy i można go zaprogramować.

Należy w tym celu postępować w następujący sposób:

- Przygotuj tabelę, w której zapiszesz wszystkie ustawienia, a także nazwy użytkowników, numery PIN i numery transponderów, które mają otrzymać dostęp za pomocą systemu kontroli dostępu.
- Jeśli chcesz utworzyć transponder główny (za jego pomocą można szybko i łatwo przejść do trybu programowania i usuwania), musisz najpierw przywrócić system kontroli dostępu do ustawień fabrycznych. Informacje na ten temat można znaleźć w rozdziale [„12.3 Resetowanie wszystkich ustawień do ustawień fabrycznych: programowanie transpondera głównego” na stronie 17](#).
- Wymyśl kod główny (powinien składać się z 6 cyfr) i zaprogramuj go. W ustawieniach fabrycznych (lub po zresetowaniu systemu kontroli dostępu) kodem głównym jest „123456”. Informacje na ten temat można znaleźć w rozdziale [„12.5 Zmiana kodu głównego” na stronie 19](#).
- W razie potrzeby zaprogramuj główny odcisk palca (umożliwia on szybki i łatwy dostęp do trybu programowania i usuwania). Informacje na ten temat można znaleźć w rozdziale [„12.6 Programowanie/usuwanie głównego odcisku palca” na stronie 19](#).
- Wybierz żądany tryb dostępu. Informacje na ten temat można znaleźć w rozdziale [„12.11 Wybór trybu dostępu” na stronie 23](#).
- Ustaw czas aktywacji styku przełącznego, który ma być używany na przykład do przełączania zamka drzwi (ustawienie domyślne to 5 sekund). Informacje na ten temat można znaleźć w rozdziale [„12.19 Ustawianie czasu aktywacji dla styku przełącznego” na stronie 34](#).
- W razie potrzeby aktywuj zabezpieczenie przed błędnymi wpisami. Szczegółowe informacje na ten temat zawierają rozdziały [„12.20 Aktywacja lub dezaktywacja zabezpieczenia przed błędnymi wpisami” na stronie 35](#) i [„12.21 Ustawianie czasu trwania alarmu dla funkcji zabezpieczenia” na stronie 35](#).
- Można teraz zapisać kod PIN użytkownika, transponder i odciski palców w zależności od ustawionego trybu dostępu.
- Sprawdź, czy styk przełączny (i np. sterowany nim zamek drzwiowy) można aktywować za pomocą zapisanych PINów użytkownika, transponderów użytkownika lub odcisków palców użytkownika.
- **Tryb blokady:** Jeśli podłączono dwa urządzenia do pracy w trybie blokady, należy skonfigurować tryb blokady. Informacje na ten temat można znaleźć w rozdziale [„12.10 Aktywacja/dezaktywacja trybu blokady” na stronie 22](#).

12 Programowanie

12.1 Dobra praktyka

- Zantuj ustawienia. W ten sposób nawet po długim czasie możesz prześledzić cały proces programowania i w razie potrzeby dostosować do nowych potrzeb.
- Zantuj dane dostępowe, takie jak nazwa użytkownika, numer miejsca w pamięci, PIN użytkownika, numer transpondera itp. aby wiedzieć, kto ma dostęp do systemu. Dane te ułatwiają również usuwanie poszczególnych kodów PIN użytkownika, transponderów użytkownika lub odcisków palców użytkownika.

12.2 Ogólne informacje

System kontroli dostępu można oczywiście przywrócić do ustawień fabrycznych – wszystkie ustawienia zostaną przy tym utracone (zapisane numery PIN, transpondery i odciski palców pozostaną w tym wypadku zapisane i mogą wymagać osobnego usunięcia).

Do programowania używa się głównie klawiatury.

Transpondera głównego lub głównego odcisku palca można również użyć do programowania lub usuwania PINów użytkowników/ transponderów użytkowników/ odcisków palców użytkowników.

System kontroli dostępu umożliwia zapisanie do 10 numerów PIN lub transponderów „gości”. Dla każdego PINu/ transpondera gościa można zaprogramować, po ilu próbach dostępu (można ustawić od 1 do 10 prób) PIN/transponder straci ważność.

→ Można na przykład zaprogramować transponder gościa tak, aby przyznawał dostęp tylko raz. Następnie jest on automatycznie usuwany z pamięci systemu kontroli dostępu i staje się tym samym nieważny.

Dla transponderów i odcisków palców przewidziano 1000 miejsc w pamięci:

- Numer miejsca w pamięci 0–98: Odciski palców użytkowników
- Numer miejsca w pamięci 99: Główny odcisk palca
- Numer miejsca w pamięci 100–987: PINy użytkowników i/lub transpondery użytkowników (w zależności od trybu dostępu)
- Numer miejsca w pamięci 988 lub 989: Grupy użytkowników antynapadowych
- Numer miejsca w pamięci 990–999: PINy gości lub transpondery gości
- System kontroli dostępu wyłącza automatycznie podświetlenie przycisków, jeśli przez 20 sekund nie zostanie wykryty żaden dotyk pola czujnika. **Pierwsze** dotknięcie pola czujnika aktywuje jedynie podświetlenie i jest rozpoznawane jako wpis; w takim wypadku system kontroli dostępu nie emituje żadnego sygnału dźwiękowego.
- Po każdym ważnym naciśnięciu przycisku system kontroli dostępu emituje krótki sygnał dźwiękowy celem potwierdzenia. Po dokonaniu prawidłowego wpisu emitowany jest dłuższy sygnał dźwiękowy, a dioda LED zaświeca się na krótko na zielono w celu potwierdzenia.
- W przypadku błędnego wpisu system kontroli dostępu emituje 3 krótkie sygnały dźwiękowe, a czerwona dioda LED miga 3-krotnie.

12.3 Resetowanie wszystkich ustawień do ustawień fabrycznych; programowanie transpondera głównego

Dzięki transponderowi głównemu można bardzo łatwo rozpocząć proces programowania lub usuwania PINów użytkownika, transponderów użytkownika lub odcisków palców użytkownika bez konieczności osobnego wywoływania trybu programowania.

➔ Ze względów bezpieczeństwa utworzenie transpondera głównego jest możliwe tylko podczas resetowania systemu kontroli dostępu do ustawień fabrycznych.

Możliwe jest również **nieutworzenie** żadnego transpondera głównego (np. jeśli ze względów bezpieczeństwa chcesz programować/usuwać PINy/ transpondery/ odciski palca użytkowników wyłącznie poprzez tryb programowania, a nie poprzez transponder główny).

12.3.1 Resetowanie systemu kontroli dostępu i programowanie transpondera głównego

➔ W danym momencie może być zarejestrowany tylko **jeden** transponder główny. Jeśli transponder główny byłby już zaprogramowany, jest on automatycznie usuwany w wyniku zaprogramowania innego transpondera.

- Wyłącz system kontroli dostępu i poczekaj, aż zgaśnie dioda LED.
- Naciśnij i przytrzymaj przycisk automatu do otwierania drzwi podłączony do systemu kontroli dostępu.
- Podłącz system kontroli dostępu ponownie do zasilania. System kontroli dostępu wyemituje 2 sygnały dźwiękowe. Teraz zwolnij przycisk automatu do otwierania drzwi.
- System kontroli dostępu wyemituje sygnał dźwiękowy, a dioda LED zaświeci się na żółto.
- Przytrzymaj transponder, który chcesz zaprogramować jako transponder główny, przed czujnikiem RFID. Po rozpoznaniu transpondera system kontroli dostępu wyemituje sygnał dźwiękowy i nastąpi zapis transpondera jako transpondera głównego.

➔ Jeśli stosowany transponder jest już zaprogramowany jako transponder użytkownika, nie można go używać jako transpondera głównego. System kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED będzie migać na czerwono.

- Dioda LED świeci się na czerwono, system kontroli dostępu znajduje się w trybie gotowości. Wszystkie ustawienia zostały zresetowane do ustawień fabrycznych.

12.3.2 Resetowanie systemu kontroli dostępu bez programowania transpondera głównego

➔ Opisana poniżej procedura umożliwia obsługę systemu kontroli dostępu bez transpondera głównego. Umożliwia ona również usunięcie istniejącego transpondera głównego, np. w przypadku jego utraty.

- Wyłącz system kontroli dostępu i poczekaj, aż zgaśnie dioda LED.
- Naciśnij i przytrzymaj przycisk automatu do otwierania drzwi podłączony do systemu kontroli dostępu.
- Włącz system kontroli dostępu ponownie. System kontroli dostępu wyemituje 2 sygnały dźwiękowe.
- Odczekaj około 5 sekund, trzymaj nadal przciśnięty przycisk automatu do otwierania drzwi, nie zwalnij go.
- System kontroli dostępu wyemituje sygnał dźwiękowy, a dioda LED zaświeci się na czerwono.
- Można teraz zwolnić przycisk otwierania drzwi, aby system kontroli dostępu mógł powrócić do trybu gotowości. Wszystkie ustawienia zostały zresetowane do ustawień fabrycznych; **nie** istnieje żaden transponder główny.

12.3.3 Przegląd ustawień standardowych

Funkcja	Ustawienie po zresetowaniu do ustawień fabrycznych
Kod główny	123456
Główny odcisk palca	pozostaje zapisany/nie jest usuwany
PINy/ transpondery/ odciski palców użytkowników lub gości	pozostają zapisane/nie są usuwane
Tryb	77 (zastosowanie jako system kontroli dostępu lub jako sterownik Wiegand)
Szybkość przesyłania danych Wiegand	26 bitów
Bit parzystości Wiegand	Wł.
Format wyjściowy w przypadku stosowania jako czytnik kart Wiegand	4 bity
Alarm w przypadku 10-krotnego błędnego wpisu	Wyl.
Czas trwania alarmu w przypadku 10-krotnego błędnego wpisu	1 minuta
Sygnal dźwiękowy przy naciśnięciu przycisku	Wł.
Dioda LED stanu	Wł.
Podświetlenie przycisków	Automatyczne wyłączenie po 20 sekundach bezczynności
Czas trwania aktywacji wyjścia przełączającego	5 sekund
Aktywacja wyjścia	Dostęp w przypadku prawidłowego PINu lub transpondera lub odcisku palca
Automatyczne programowanie nowych transponderów	Wyl.

12.4 Aktywacja/dezaktywacja trybu programowania

- Aby rozpocząć tryb programowania, wprowadź 6-cyfrowy kod główny w następujący sposób (ustawienie domyślne = 123456):

✱ 1 2 3 4 5 6 ✱

- Dioda LED miga wtedy na czerwono (tryb programowania jest aktywny). Teraz można np. programować/usuwać PINy/transpondery użytkowników lub dokonywać różnych ustawień.
- Aby wyjść z trybu programowania (miga czerwona dioda LED), naciśnij przycisk ✱. System kontroli dostępu przejdzie wtedy ponownie w tryb gotowości, dioda LED będzie się świecić stale na czerwono.

➔ Jeśli aktywujesz tryb programowania i nie naciśniesz żadnego przycisku przez 30 sekund, tryb programowania zostanie automatycznie dezaktywowany ze względów bezpieczeństwa, a system kontroli dostępu powróci do trybu gotowości. Zostanie zastosowane wcześniej zakończone programowanie.

12.5 Zmiana kodu głównego

Kod główny jest wymagany do całego programowania systemu kontroli dostępu i dlatego należy go odpowiednio wybrać.

W ustawieniach domyślnych (lub po zresetowaniu zamka kodowego) kod główny to „123456”. Ze względów bezpieczeństwa zalecamy zmianę tego kodu głównego najpóźniej po zakończeniu programowania i rozpoczęciu normalnego użytkowania systemu kontroli dostępu.

➔ Kod główny musi być zawsze 6-cyfrowy.

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.
- Wprowadź kod programowania [0] dla kodu głównego. Następnie dioda LED zaświeci się na żółto.
- Następnie wprowadź nowy kod główny, np.: [9] [8] [7] [6] [5] [4]
- Potwierdź to przyciskiem [#].
- Ponownie wprowadź nowy kod główny, np.: [9] [8] [7] [6] [5] [4]
- Potwierdź to przyciskiem [#].
- Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.6 Programowanie/usuwanie głównego odcisku palca

W systemie kontroli dostępu można zaprogramować jeden główny odcisk palca. Za jego pomocą można szybko zaprogramować lub usunąć PINy, transpondery lub odciski palców użytkowników.

➔ Numer miejsca 99 w pamięci jest zarezerwowany dla głównego odcisku palca.

12.6.1 Programowanie głównego odcisku palca

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.
- Wprowadź kod programowania [1], aby rozpocząć proces programowania. Następnie dioda LED zaświeci się na żółto.
- Wprowadź numer miejsca w pamięci [9] [9] dla głównego odcisku palca.
- Potwierdź to przyciskiem [#].

➔ Jeśli do numeru miejsca w pamięci 99 jest już przypisany główny odcisk palca, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED zamiga 3-krotnie na czerwono. Nadpisanie istniejącego głównego odcisku palca nie jest tym samym możliwe. Najpierw należy usunąć miejsce 99 w pamięci (patrz niżej), zanim będzie można pod nim zapisać kolejny główny odcisk palca.

- W celu zaprogramowania głównego odcisku palca czujnik linii papilarnych musi zostać dotknięty 3x tym samym palcem. Pierścień LED wokół czujnika zaświeci się na niebiesko po dotknięciu czujnika. Jeśli odcisk palca zostanie prawidłowo rozpoznany, pierścień LED zaświeci się na zielono i rozlegnie się krótki sygnał dźwiękowy.

Po trzecim poprawnym procesie odczytu system kontroli dostępu wyemituje dłuższy sygnał dźwiękowy, odcisk palca jest zapisany. Dioda LED świeci się na żółto.

➔ Jeśli poprawny odczyt odcisku palca nie jest możliwy, rozlegną się 3 sygnały dźwiękowe, a pierścień LED zamiga 3-krotnie na czerwono. To samo stanie się w przypadku próby zaprogramowania już zapisanego odcisku palca.

- Naciśnij przycisk [#], aby wyjść z trybu programowania.
- Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.7 Usuwanie głównego odcisku palca

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.
- Wprowadź kod programowania [2], aby aktywować tryb usuwania. Następnie dioda LED zaświeci się na żółto.
- Wprowadź numer miejsca w pamięci [9] [9] dla głównego odcisku palca.
- Potwierdź to przyciskiem [#].

➔ Jeżeli miejsce w pamięci jest już puste, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED będzie migać na czerwono.

- Wyjdź z trybu usuwania przyciskiem [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.8 Ustawianie trybu pracy dla złącza Wiegand

System kontroli dostępu może działać jako zewnętrzny czytnik dla sterownika Wiegand lub jako sterownik Wiegand dla czytnika zewnętrznego. Żądany tryb można ustawić w systemie kontroli dostępu.

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.
- Wprowadź kod programowania [7], aby uruchomić tryb ustawień. Następnie dioda LED zaświeci się na żółto.
- Wybierz żądaną funkcję:

[7] = system kontroli dostępu funkcjonuje jako sterownik Wiegand lub jako system samodzielny (ustawienie fabryczne)

[8] = system kontroli dostępu funkcjonuje jako czytnik dla zewnętrznego sterownika Wiegand

- Naciśnij przycisk [#], aby wyjść z trybu ustawień. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

➔ Jeśli system kontroli dostępu ma funkcjonować jako system samodzielny (bez dodatkowego czytnika zewnętrznego), należy zastosować ustawienie fabryczne ([7]).

Jeśli system kontroli dostępu funkcjonuje jako czytnik ([8]), nie działają prawie wszystkie ustawienia systemu kontroli dostępu, ponieważ przejmuje je zewnętrzny sterownik Wiegand. Żółty przewód przyłączeniowy w systemie kontroli dostępu nie aktywuje już przycisku automatu do otwierania drzwi i może być używany do sterowania sygnalizatorem dźwiękowym w systemie kontroli dostępu (niski sygnał = sygnał dźwiękowy aktywny).

12.9 Konfigurowanie rozpoznawania otwarcia drzwi

Skonfiguruj rozpoznawanie otwarcia drzwi, aby otrzymywać ostrzeżenie, jeśli drzwi pozostaną otwarte dłużej niż ustawiony czas lub jeśli drzwi zostaną otwarte siłą. Rozpoznawanie otwarcia drzwi działa tylko w przypadku podłączenia dodatkowego zestyku magnetycznego lub użycia wbudowanego zestyku magnetycznego.

Mechanizm	Opis
Drzwi pozostają otwarte dłużej niż czas ustawiony na timerze	Jeśli drzwi pozostaną otwarte dłużej niż czas ustawiony na timerze, włączy się wbudowany brzęczyk. Zamknięcie drzwi powoduje wyłączenie brzęczyka.
Drzwi są otwierane	Po otwarciu drzwi wbudowany brzęczyk emituje dźwięk przez określony czas (ustawienie timera) i uruchamiany jest podłączony system alarmowy (jeśli jest dostępny). Alarm jest wyłączany po upływie czasu ustawionego na timerze. Alarm może zostać wyłączony przez upoważnioną osobę.

Aktywacja/dezaktywacja rozpoznawania otwarcia drzwi

Wszystkie mechanizmy są aktywowane lub dezaktywowane jednocześnie. Ustawiony timer dotyczy obu mechanizmów.

Aktywacja rozpoznawania	Dezaktywacja rozpoznawania	Kombinacja przycisków/obsługa
1. Aktywacja trybu programowania	1. Aktywacja trybu programowania	[*] (kod główny) #
	2. Dezaktywacja rozpoznawania otwarcia drzwi	[6] [3] #
2. Aktywacja rozpoznawania otwarcia drzwi		[6] [4] #
3. Ustawianie timera		[5] (0 ... [3]) # (0, [1] = 1 minuta, [3] = 3 minuty) Wyłącza każdy alarm poprzez ustawienie timera na 0.
4. Wychodzenie z trybu programowania	3. Wychodzenie z trybu programowania	[*]

Dezaktywacja alarmów

Mechanizm	Dezaktywacja alarmów
Drzwi pozostają otwarte dłużej niż ustawiony próg czasowy	■ Zamknij drzwi. ■ Użyj zarejestrowanego transpondera głównego/standardowego, odcisku palca głównego/standardowego, kodu PIN głównego/standardowego, aby aktywować system kontroli dostępu (otworzyć drzwi).
Drzwi są otwierane	■ Użyj zarejestrowanego transpondera głównego/standardowego, odcisku palca głównego/standardowego, kodu PIN głównego/standardowego, aby aktywować system kontroli dostępu (otworzyć drzwi).

12.10 Aktywacja/dezaktywacja trybu blokady

W przypadku połączenia ze sobą dwóch systemów kontroli dostępu do pracy w trybie blokady, należy aktywować tryb blokady w obu systemach kontroli dostępu.

Aktywacja

Kroki	Kombinacja przycisków/obsługa
1. Skonfiguruj ustawienia w pierwszym systemie kontroli dostępu.	Skonfiguruj kody PIN, odciski palca i transpondery na jednym urządzeniu.
2. Przenieś ustawienia pierwszego systemu kontroli dostępu do drugiego systemu kontroli dostępu.	Więcej informacji znajduje się w rozdziale „ 12.26 Transmisja danych pomiędzy dwoma systemami kontroli dostępu ” na stronie 40.
3. Aktywuj tryb programowania na obu urządzeniach.	* (kod główny) #
4. Aktywuj tryb blokowania na obu urządzeniach.	9 0 # (ustawienie fabryczne)
5. Wyjdź z trybu programowania.	*
6. Przetestuj tryb blokady.	1. Otwórz pierwsze drzwi sterowane przez system kontroli dostępu. 2. Poczekaj, aż pierwsze drzwi zostaną zamknięte. 3. Otwórz drugie drzwi sterowane przez drugi system kontroli dostępu.

Dezaktywacja

Kroki	Kombinacja przycisków/obsługa
1. Aktywuj tryb programowania na obu urządzeniach.	* (kod główny) #
2. Dezaktywuj tryb blokowania na obu urządzeniach.	9 1 # (ustawienie fabryczne)
3. Wychodzenie z trybu programowania	*

12.11 Wybór trybu dostępu

System kontroli dostępu oferuje różne możliwości aktywacji styku przełącznego:

- Tylko przy pomocy odcisku palca
- Tylko przy pomocy transpondera
- Tylko przy pomocy PINu
- Przy pomocy PINu , transpondera **lub** odcisku palca (ustawienie domyślne)
- Tylko przy pomocy 2–9 transponderów (dostęp jest tu przyznawany np. tylko wtedy, gdy obecnych jest kilka osób i podejmują próbę dostępu bezpośrednio jedna po drugiej (maks. 5 sekund na każdą osobę), np. w przypadku pomieszczeń o szczególnym znaczeniu dla bezpieczeństwa – w ten sposób osoba samotna nie otrzyma dostępu mimo ważnego transpondera).

→ Przy pomocy transpondera głównego lub głównego odcisku palca nie można zasadniczo aktywować styku przełącznego systemu kontroli dostępu.

Należy postępować w następujący sposób:

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.
- Wprowadź kod programowania [4] dla trybu dostępu. Następnie dioda LED zaświeci się na żółto.
- Wybierz żądany tryb dostępu:

[0] = tylko za pomocą odcisku palca

[1] = tylko za pomocą transpondera

[2] = tylko za pomocą PINu

[3] + ([2] [9]) = dostęp dla wielu użytkowników

Przykład: [3] [4] = styk przełączny aktywuje się i przyznawany jest dostęp tylko wtedy, gdy 4 osoby bezpośrednio jedna po drugiej podejmą ważną próbę dostępu za pomocą transpondera w ciągu maksymalnie 5 sekund na osobę

[4] = za pomocą PINu , transpondera **albo** odcisku palca (ustawienie domyślne)

- Wyjdź z trybu ustawień za pomocą przycisku [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.12 Zapisywanie PINu użytkownika

System kontroli dostępu posiada 888 miejsc w pamięci do zapisywania kodów PIN użytkownika i/lub transponderów użytkownika. Miejsca w pamięci o numerach od 100 do 987 są przeznaczone dla kodów PIN/transponderów.

Do zapisywania można użyć klawiatury, transpondera głównego lub głównego odcisku palca.

→ Zalecamy utworzenie tabeli i wprowadzenie wszystkich danych dostępu, takich jak nazwa użytkownika, numer miejsca w pamięci, kod PIN użytkownika, numer transpondera itp. Umożliwia to prześledzenie, kto miał dostęp do systemu kontroli dostępu i korzystał z określonego miejsca w pamięci.

Bardzo łatwo można też usunąć konkretnego użytkownika, który nie ma już posiadać prawa dostępu lub który zapomniał swojego kodu PIN użytkownika albo zgubił swój transponder użytkownika.

W przeciwnym razie mogłoby być konieczne usunięcie wszystkich miejsc w pamięci i rozpoczęcie wszystkiego od nowa.

Przy zapisywaniu PINu użytkownika można postępować na dwa różne sposoby:

- Zapisanie PINu użytkownika w następnym wolnym miejscu w pamięci
- Zapisanie PINu użytkownika w określonym miejscu w pamięci

12.12.1 Automatyczne zapisanie PINu użytkownika w następnym wolnym miejscu w pamięci

→ Ten tryb zapisywania umożliwia szybkie i łatwe programowanie nowych kodów PIN użytkownika w następnym wolnym miejscu w pamięci.

Jednak usunięcie konkretnego PINu użytkownika jest w tym przypadku możliwe tylko poprzez sam PIN – ponieważ przyporządkowanie pomiędzy PINem użytkownika a numerem miejsca w pamięci jest nieznane. W takim przypadku wszystkie miejsca w pamięci musiałyby zostać usunięte.

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.
- Wprowadź kod programowania [1], aby aktywować tryb zapisywania. Następnie dioda LED zaświeci się na żółto.

→ Alternatywnie do tych czynności można przytrzymać transponder główny 1x przed powierzchnią odczytu – lub dotknąć czujnika linii papilarnych 1x głównym odciskiem palca. Obydwie metody aktywują tryb zapisywania, dioda LED świeci się na żółto.

- Teraz wprowadź żądany PIN użytkownika i potwierdź wpis przyciskiem [#].

Przykład: [2][2][2][2][#] = zapis PINu użytkownika 2222

→ PIN użytkownika może być 4–6-cyfrowy. Jednak kombinacja liczb 8888 nie jest możliwa, ponieważ jest to kombinacja serwisowa (standardowy kod użytkownika).

Jeśli dany PIN znajduje się już w jednym z miejsc w pamięci, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED będzie migać na czerwono. Ten sam kod PIN można nadać tylko raz.

- W razie potrzeby można zapisać kolejne PINy użytkowników. Wprowadź po prostu żądany 4- ... 6-cyfrowy PIN użytkownika i potwierdź go przyciskiem [#].
- Wyjdź z trybu zapisywania przyciskiem [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.12.2 Przypisanie PINu użytkownika do określonego miejsca w pamięci

→ Proces ten trwa wprawdzie dłużej, ale za to później określony PIN użytkownika można usunąć (poprzez numer miejsca w pamięci), nawet jeśli został zapomniany (pod warunkiem, że utworzono tabelę z danymi dostępowymi zgodnie z zaleceniami z początku rozdziału).

- Aktywuj tryb programowania zgodnie z opisem w „12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18; dioda LED zacznie migać na czerwono.

- Wprowadź kod programowania [1], aby aktywować tryb zapisywania. Następnie dioda LED zaświeci się na żółto.

→ Alternatywnie do tych czynności można przytrzymać transponder główny 1x przed powierzchnią odczytu – lub dotknąć czujnika linii papilarnych 1x głównym odciskiem palca. Obydwie metody aktywują tryb zapisywania, dioda LED świeci się na żółto.

- Wprowadź numer miejsca w pamięci ([1] [0] [0] [9] [8] [7]), pod którym ma być zapisany PIN użytkownika i potwierdź wpis przyciskiem [#].

Przykład: [6] [5] [4] [#] = zapis PINu użytkownika pod numerem miejsca w pamięci 654

→ Jeśli dany numer miejsca w pamięci jest już nadany, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED będzie migać na czerwono.

- Teraz wprowadź żądany PIN użytkownika i potwierdź wpis przyciskiem [#].

Przykład: [2] [2] [2] [2] [#] = zapis PINu użytkownika 2222

→ PIN użytkownika może być 4–6-cyfrowy. Jednak kombinacja liczb 8888 nie jest możliwa, ponieważ jest to kombinacja serwisowa (standardowy kod użytkownika).

Jeśli dany PIN znajduje się już w jednym z miejsc w pamięci, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED będzie migać na czerwono. Ten sam kod PIN można nadać tylko raz.

- W razie potrzeby można zapisać kolejne PINy użytkowników. Wprowadź po prostu 3-cyfrowy numer miejsca w pamięci ([1] [0] [0] [9] [8] [7]) i potwierdź go przyciskiem [#]. Następnie wprowadź żądany 4–6-cyfrowy PIN użytkownika i potwierdź go przyciskiem [#].

- Wyjdź z trybu zapisywania przyciskiem [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [X].

12.13 Usuwanie PINu użytkownika

Dany użytkownik nie otrzymuje już dostępu za pośrednictwem swojego kodu PIN użytkownika, jeśli odpowiedni kod PIN użytkownika został usunięty.

Przy usuwaniu PINu użytkownika można postępować na dwa różne sposoby:

- Usunąć kod PIN użytkownika.
- Usunąć miejsce w pamięci, pod którym zapisany jest kod PIN użytkownika.

12.13.1 Usuwanie PINu użytkownika

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.

- Wprowadź kod programowania [2], aby uruchomić tryb usuwania. Następnie dioda LED zaświeci się na żółto.

→ Alternatywnie do tych czynności można przytrzymać transponder główny 2x przed powierzchnią odczytu – lub dotknąć czujnika linii papilarnych 2x głównym odciskiem palca (każdorazowo w ciągu 5 sekund). Obydwie metody aktywują tryb usuwania, dioda LED świeci się na żółto.

- Wprowadź PIN użytkownika, który chcesz usunąć, i potwierdź wpis przyciskiem [#]. PIN użytkownika jest usuwany.

Przykład: [6] [5] [4] [3] [#] = zapis PINu użytkownika 6543

- W razie potrzeby można teraz usunąć kolejne kody PIN użytkownika (wprowadź żądany kod PIN użytkownika i naciśnij przycisk [#] w celu potwierdzenia).

→ Jeśli PIN użytkownika jest nieznanym i/lub już usuniętym, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED będzie migać na czerwono.

- Wyjdź z trybu usuwania przyciskiem [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.13.2 Usuwanie PINu użytkownika za pomocą numeru miejsca w pamięci

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.

- Wprowadź kod programowania [2], aby uruchomić tryb usuwania. Następnie dioda LED zaświeci się na żółto.

→ Alternatywnie do tych czynności można przytrzymać transponder główny 2x przed powierzchnią odczytu – lub dotknąć czujnika linii papilarnych 2x głównym odciskiem palca (każdorazowo w ciągu 5 sekund). Obydwie metody aktywują tryb usuwania, dioda LED świeci się na żółto.

- Wprowadź 3-cyfrowy numer miejsca w pamięci ([1] [0] [0] [9] [8] [7]), który chcesz usunąć, i potwierdź wpis przyciskiem [#]. Numer miejsca w pamięci (z zapisanymi w nim danymi) jest usuwany.

Przykład: [6] [5] [4] [#] = usuwanie numeru miejsca w pamięci 654

→ Jeżeli dany numer miejsca w pamięci jest już pusty, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED będzie migać na czerwono.

- W razie potrzeby można teraz usunąć kolejne numery miejsc w pamięci (wprowadź numer miejsca w pamięci i naciśnij przycisk [#] w celu potwierdzenia).

- Wyjdź z trybu usuwania przyciskiem [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.14 Programowanie transpondera użytkownika

System kontroli dostępu posiada 888 miejsc w pamięci do zapisywania kodów PIN użytkownika i/lub transponderów użytkownika. Miejsca w pamięci o numerach od 100 do 987 są przeznaczone dla kodów PIN/transponderów.

Do zapisywania można użyć klawiatury, transpondera głównego lub głównego odcisku palca.

→ Zalecamy utworzenie tabeli i wprowadzenie wszystkich danych dostępu, takich jak nazwa użytkownika, numer miejsca w pamięci, kod PIN użytkownika, numer transpondera itp. Umożliwia to prześledzenie, kto miał dostęp do systemu kontroli dostępu i korzystał z określonego miejsca w pamięci.

Bardzo łatwo można też usunąć konkretnego użytkownika, który nie ma już posiadać prawa dostępu, lub gdy zagubiono transponder użytkownika albo gdy jest on uszkodzony.

W przeciwnym razie mogłoby być konieczne usunięcie wszystkich miejsc w pamięci i rozpoczęcie wszystkiego od nowa.

Przy programowaniu można postępować na trzy różne sposoby:

- Szybkie zaprogramowanie transpondera użytkownika w następnym wolnym miejscu w pamięci
- Programowanie transpondera użytkownika w określonym miejscu w pamięci
- Programowanie kilku transponderów użytkownika z kolejnym numerem transpondera

12.14.1 Automatyczne zapisanie transpondera użytkownika w kolejnym wolnym miejscu w pamięci

→ Ten tryb programowania umożliwia szybkie i łatwe programowanie nowych transponderów użytkownika w następnym wolnym miejscu w pamięci.

Jednak usunięcie konkretnego transpondera użytkownika jest w tym przypadku możliwe tylko poprzez sam transponder, ponieważ przyporządkowanie pomiędzy transponderem użytkownika a numerem miejsca w pamięci jest nieznanne. W takim przypadku wszystkie miejsca w pamięci musiałyby zostać usunięte.

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.
- Wprowadź kod programowania [1], aby aktywować tryb zapisywania. Następnie dioda LED zaświeci się na żółto.

→ Alternatywnie do tych czynności można przytrzymać transponder główny 1x przed powierzchnią odczytu – lub dotknąć czujnika linii papilarnych 1x głównym odciskiem palca. Obydwie metody aktywują tryb zapisywania, dioda LED świeci się na żółto.

- Przytrzymaj transponder przed czujnikiem RFID. Po rozpoznaniu nowego transpondera system kontroli dostępu wyemituje krótki sygnał dźwiękowy i nastąpi zapis transpondera.

Zamiast trzymać transponder przed czujnikiem RFID można wprowadzić 8- lub 10-cyfrowy numer transpondera i potwierdzić przyciskiem [#].

Przykład: 0 0 0 3 1 7 1 4 5 6 [#]

→ Jeśli transponder został już zaprogramowany, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED będzie migać na czerwono. Tym samym wielokrotne programowanie tego samego transpondera nie jest możliwe.

- Można również zaprogramować kolejne transpondery, postępując w sposób opisany powyżej wystarczy przytrzymać transponder przed czujnikiem RFID **lub** wprowadzić numer transpondera i potwierdzić przyciskiem [#].
- Wyjdź z trybu zapisywania przyciskiem [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.14.2 Przypisanie transpondera użytkownika do określonego miejsca w pamięci

→ Ten proces programowania trwa dłużej, ale określony transponder użytkownika można później usunąć (poprzez numer miejsca w pamięci), jeśli został zagubiony lub uszkodzony.

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.
- Wprowadź kod programowania **[1]**, aby aktywować tryb zapisywania. Następnie dioda LED zaświeci się na żółto.

→ Alternatywnie do tych czynności można przytrzymać transponder główny **1x** przed powierzchnią odczytu – lub dotknąć czujnika linii papilarnych **1x** głównym odciskiem palca. Obydwie metody aktywują tryb zapisywania, dioda LED świeci się na żółto.

- Wprowadź numer miejsca w pamięci (**[1] [0] [0] [9] [8] [7]**), pod którym ma być zapisany transponder użytkownika i potwierdź numer miejsca w pamięci przyciskiem **[#]**.

Przykład: **[6] [5] [4] [#]** = zapis transpondera pod numerem miejsca w pamięci 654

→ Jeśli dany numer miejsca w pamięci jest już zajęty, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED będzie migać na czerwono. Nadpisanie miejsca w pamięci jest tym samym niemożliwe. Najpierw należy usunąć dany numer miejsca w pamięci, zanim będzie można zapisać pod nim transponder użytkownika.

- Przytrzymaj transponder przed czujnikiem RFID. Po rozpoznaniu nowego transpondera system kontroli dostępu wyemituje krótki sygnał dźwiękowy i nastąpi zapis transpondera.

Zamiast trzymać transponder przed czujnikiem RFID można wprowadzić 8- lub 10-cyfrowy numer transpondera i potwierdzić przyciskiem **[#]**.

Przykład: **[0] [0] [0] [3] [1] [7] [1] [4] [5] [6] [#]**

→ Jeśli parowanie transpondera jest już ukończone, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED będzie migać na czerwono. Tym samym wielokrotne parowanie tego samego transpondera nie jest możliwe.

- Jeżeli chcesz zaprogramować kolejny transponder użytkownika, zacznij ponownie od wprowadzenia numeru miejsca w pamięci, patrz wyżej.
- Wyjdź z trybu parowania przyciskiem **[#]**. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem **[*]**.

12.14.3 Programowanie kilku transponderów użytkownika z kolejnym numerem transpondera

Ta opcja umożliwia jednoczesne zapisanie kilku transponderów z kolejnymi numerami transponderów (składającymi się z 8 lub 10 cyfr) przy użyciu opcji zapisu masowego.

→ Ponieważ numery miejsc w pamięci są również kolejne, możliwe jest przyporządkowanie transponderów do numerów miejsc w pamięci, a tym samym usunięcie pojedynczego transpondera poprzez numer miejsca w pamięci w przypadku jego zagubienia lub uszkodzenia.

Warunkiem wstępnym jest oczywiście utworzenie listy z numerami transponderów i numerami miejsc w pamięci. Ponadto żadne miejsce w pamięci biorące udział w procesie zapisu masowego nie może być zajęte; w przeciwnym razie zajęte miejsce w pamięci zostanie pominięte podczas zapisu masowego, a wszystkie kolejne przyporządkowania między transponderami i numerami miejsc w pamięci zostaną odpowiednio przesunięte.

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.
- Wprowadź kod programowania **[1]**, aby aktywować tryb zapisywania. Następnie dioda LED zaświeci się na żółto.
- Wprowadź numer miejsca w pamięci (**[1] [0] [0] [9] [8] [7]**), od którego ma nastąpić zapis masowy i potwierdź wpis przyciskiem **[#]**.

Przykład: **[3] [0] [0] [#]** = pierwsze miejsce w pamięci dla zapisu masowego

→ Jeśli ten numer miejsca w pamięci jest już zajęty, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED będzie migać na czerwono.

- Wprowadź liczbę transponderów, które chcesz zapisać poprzez zapis masowy i potwierdź wpis przyciskiem [#].

Przykład: [1][0][0][#] = ma nastąpić zapis 100 transponderów z kolejnymi numerami

→ Upewnij się, że od wprowadzonego numeru miejsca w pamięci dostępna jest jeszcze dostateczna ilość miejsc w pamięci stosownie do zapisywanej liczby transponderów. W takim wypadku system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED będzie migać na czerwono.

- Wprowadź numer pierwszego transpondera (8- lub 10-cyfrowy) i potwierdź go przyciskiem [#].

Przykład: [0][0][0][3][1][7][1][4][5][6][#]

- Następnie system kontroli dostępu zapisuje wprowadzoną liczbę transponderów użytkowników w miejscu w pamięci. Proces ten może trwać do 2 minut w zależności od liczby transponderów.

- Wyjdź z trybu parowania przyciskiem [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.14.4 Programowanie transponderów użytkowników w trybie zbiorczym

Jeżeli tryb ten jest aktywny, każdy transponder może aktywować styk przełączny. Jednocześnie transponder zostaje automatycznie zapisany w kolejnym wolnym miejscu w pamięci jako transponder użytkownika.

→ Ten tryb parowania umożliwia szybkie i łatwe parowanie nowych transponderów użytkownika w następnym wolnym miejscu w pamięci.

Jednak usunięcie konkretnego transpondera użytkownika jest w tym przypadku możliwe tylko poprzez sam transponder, ponieważ przyporządkowanie pomiędzy transponderem użytkownika a numerem miejsca w pamięci jest nieznanne. W takim przypadku wszystkie miejsca w pamięci musiałyby zostać usunięte, jeśli tylko jeden transponder miałby nie mieć już dostępu.

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.

- Wprowadź kod programowania [9]. Następnie dioda LED zaświeci się na żółto.

- Wybierz żądaną funkcję:

[2] = tryb zbiorczy wyłączony (ustawienie fabryczne)

[3] = tryb zbiorczy włączony

- Wyjdź z trybu ustawień za pomocą przycisku [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

→ Jeśli włączony jest tryb zbiorczy, każdy transponder aktywuje styk przełączny. Jednocześnie transponder zostaje automatycznie zapisany w kolejnym wolnym miejscu w pamięci jako transponder użytkownika.

Jeśli ponownie przytrzymasz zaprogramowany już transponder przed czujnikiem RFID, nie zostanie on zapisany ponownie (ale styk przełączny zostanie aktywowany).

Pamiętaj koniecznie o ponownym wyłączeniu trybu zbiorczego, gdy nie będzie już potrzebny. W przeciwnym razie każda osoba trzymająca transponder przed czujnikiem RFID w systemie kontroli dostępu może uzyskać dostęp.

12.15 Usuwanie transpondera użytkownika

Gdy tylko odpowiedni transponder użytkownika zostanie usunięty, dany użytkownik nie będzie już mieć dostępu.

Przy usuwaniu transpondera użytkownika można postępować na trzy różne sposoby:

- Usunięcie transpondera użytkownika poprzez odczyt.
- Usunięcie transpondera użytkownika za pomocą numeru transpondera.
- Usunięcie miejsca w pamięci, pod którym zapisany jest transponder.

12.15.1 Usuwanie transpondera użytkownika za pomocą transpondera

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.

- Wprowadź kod programowania [2], aby uruchomić tryb usuwania. Następnie dioda LED zaświeci się na żółto.

→ Alternatywnie do tych czynności można przytrzymać transponder główny 2x przed powierzchnią odczytu – lub dotknąć czujnika linii papilarnych 2x głównym odciskiem palca (każdorazowo w ciągu 5 sekund). Obydwie metody aktywują trybu usuwania, dioda LED świeci się na żółto.

- Przytrzymaj transponder użytkownika przed czujnikiem RFID. Po rozpoznaniu transpondera system kontroli dostępu wyemituje krótki sygnał dźwiękowy i nastąpi usunięcie transpondera.

→ Jeśli transponder użytkownika jest nieznan y i/lub już usunięty, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED zamiga 3 razy na czerwono.

- Następnie można usunąć kolejny transponder użytkownika w sposób opisany powyżej (należy go przytrzymać przed czujnikiem RFID).

- Wyjdź z trybu usuwania przyciskiem [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.15.2 Usuwanie transpondera użytkownika za pomocą numeru transpondera

Wiele transponderów ma nadrukowany 8- lub 10-cyfrowy numer. Wprowadzając ten numer, można usunąć uszkodzony transponder (np. uszkodzona karta transpondera).

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.

- Wprowadź kod programowania [2], aby uruchomić tryb usuwania. Następnie dioda LED zaświeci się na żółto.

→ Alternatywnie do tych czynności można przytrzymać transponder główny 2x przed powierzchnią odczytu – lub dotknąć czujnika linii papilarnych 2x głównym odciskiem palca (każdorazowo w ciągu 5 sekund). Obydwie metody aktywują trybu usuwania, dioda LED świeci się na żółto.

- Wprowadź 8- lub 10-cyfrowy numer transpondera i potwierdź go przyciskiem [#].

Przykład: 0 0 0 3 1 7 1 4 5 6 [#]

→ Jeśli numer transponder jest nieznan y i/lub już usunięty, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED zamiga 3 razy na czerwono.

- Następnie można usunąć kolejny transponder użytkownika w sposób opisany powyżej (wprowadzić numer transpondera i nacisnąć przycisk [#] w celu potwierdzenia).

- Wyjdź z trybu usuwania przyciskiem [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.15.3 Usuwanie transpondera użytkownika za pomocą numeru miejsca w pamięci

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.

- Wprowadź kod programowania [2], aby uruchomić tryb usuwania. Następnie dioda LED zaświeci się na żółto.

→ Alternatywnie do tych czynności można przytrzymać transponder główny 2x przed powierzchnią odczytu – lub dotknąć czujnika linii papilarnych 2x głównym odciskiem palca (každorazowo w ciągu 5 sekund). Obydwie metody aktywują trybu usuwania, dioda LED świeci się na żółto.

- Wprowadź 3-cyfrowy numer miejsca w pamięci ([1] [0] [0] [9] [8] [7]), który chcesz usunąć, i potwierdź wpis przyciskiem [#]. Numer miejsca w pamięci (z zapisanymi w nim danymi) jest usuwany.

Przykład: [6] [5] [4] [#] = usuwanie numeru miejsca w pamięci 654

→ Jeśli dany numer miejsca w pamięci jest już pusty, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED zamiga 3-krotnie na czerwono.

- W razie potrzeby można teraz usunąć kolejne numery miejsc w pamięci (wprowadź numer miejsca w pamięci i naciśnij przycisk [#] w celu potwierdzenia).

- Wyjdź z trybu usuwania przyciskiem [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [X].

12.16 Programowanie odcisku palca użytkownika

System kontroli dostępu może zapisać do 99 różnych odcisków palca użytkownika. Przeznaczone są dla nich numery miejsc w pamięci 0–98.

Proces programowania jest możliwy zarówno za pomocą klawiatury, jak i za pomocą transpondera głównego lub głównego odcisku palca.

→ Zalecamy utworzenie tabeli i wprowadzenie wszystkich danych dostępu, takich jak nazwa użytkownika, numer miejsca w pamięci, kod PIN użytkownika, numer transpondera itp. Umożliwia to prześledzenie, kto miał dostęp do systemu kontroli dostępu i korzystał z określonego miejsca w pamięci.

Bardzo łatwo można też usunąć konkretnego użytkownika, który nie ma już posiadać prawa dostępu.

W przeciwnym razie mogłoby być konieczne usunięcie wszystkich miejsc w pamięci i rozpoczęcie wszystkiego od nowa.

Przy zapisywaniu odcisku palca użytkownika można postępować na dwa różne sposoby:

- Zapisanie odcisku palca użytkownika w następnym wolnym miejscu w pamięci
- Zapisanie odcisku palca użytkownika w określonym miejscu w pamięci

12.16.1 Automatyczne zapisanie odcisku palca użytkownika w następnym wolnym miejscu w pamięci

→ Ten tryb programowania umożliwia szybkie i łatwe programowanie nowych odcisków palca użytkownika w następnym wolnym miejscu w pamięci.

Jednak usunięcie konkretnego odcisku palca użytkownika jest w tym przypadku możliwe tylko poprzez sam odcisk palca – ponieważ przyporządkowanie pomiędzy odciskiem palca użytkownika a numerem miejsca w pamięci jest nieznanne. W takim przypadku wszystkie miejsca w pamięci musiałyby zostać usunięte.

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.

- Wprowadź kod programowania [1], aby aktywować tryb zapisywania. Następnie dioda LED zaświeci się na żółto.

→ Alternatywnie do tych czynności można przytrzymać transponder główny 1x przed powierzchnią odczytu – lub dotknąć czujnika linii papilarnych 1x głównym odciskiem palca. Obydwie metody aktywują tryb zapisywania, dioda LED świeci się na żółto.

- W celu zaprogramowania odcisku palca użytkownika czujnik linii papilarnych musi zostać dotknięty 3x tym samym palcem. Pierścień LED wokół czujnika zaświeci się na niebiesko po dotknięciu czujnika. Jeśli odcisk palca zostanie prawidłowo rozpoznany, pierścień LED zaświeci się na zielono i rozlegnie się krótki sygnał dźwiękowy. Po trzecim poprawnym procesie odczytu system kontroli dostępu emituje dłuższy sygnał dźwiękowy, a dioda LED zaświeca się na zielono, odcisk palca jest zapisany.
- Jeśli odcisk palca nie zostanie prawidłowo odczytany, rozlegną się 3 sygnały dźwiękowe, a pierścień LED zacznie migać na czerwono. To samo stanie się w przypadku próby wczytania już zapisanego odcisku palca.
- Teraz można zaprogramować kolejny odcisk palca użytkownika, postępując w sposób opisany powyżej (dotknąć czujnika linii papilarnych 3x z rzędu).
- Wyjdź z trybu parowania przyciskiem [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.16.2 Przypisywanie odcisku palca użytkownika do określonego miejsca w pamięci

- Ten proces programowania trwa dłużej, jednak określony odcisk palca użytkownika można później usunąć (poprzez numer miejsca w pamięci), nawet jeśli dana osoba nie jest już dostępna podczas procesu usuwania.
- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.
- Wprowadź kod programowania [1], aby aktywować tryb zapisywania. Następnie dioda LED zaświeci się na żółto.
- Alternatywnie do tych czynności można przytrzymać transponder główny 1x przed powierzchnią odczytu – lub dotknąć czujnika linii papilarnych 1x głównym odciskiem palca. Obydwie metody aktywują tryb zapisywania, dioda LED świeci się na żółto.
- Wprowadź numer miejsca w pamięci ([0] [9] [8]), pod którym ma być zapisany odcisk palca użytkownika (bez zera wiodącego dla jednocyfrowych numerów miejsc pamięci) i potwierdź wpis przyciskiem [#].
Przykład 1: [6] [#] = zapis odcisku palca użytkownika pod numerem miejsca w pamięci 6
Przykład 2: [5] [4] [#] = zapis odcisku palca użytkownika pod numerem miejsca w pamięci 54
- Jeśli dany numer miejsca w pamięci jest już zajęty, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED będzie migać na czerwono. Nadpisanie miejsca w pamięci jest tym samym niemożliwe. Najpierw należy usunąć dany numer miejsca w pamięci, zanim będzie można zapisać pod nim inny odcisk palca użytkownika.
- W celu zaprogramowania odcisku palca użytkownika czujnik linii papilarnych musi zostać dotknięty 3x tym samym palcem. Pierścień LED wokół czujnika zaświeci się na niebiesko po dotknięciu czujnika. Jeśli odcisk palca zostanie prawidłowo rozpoznany, pierścień LED zaświeci się na zielono i rozlegnie się krótki sygnał dźwiękowy. Po trzecim poprawnym procesie odczytu system kontroli dostępu emituje dłuższy sygnał dźwiękowy, a dioda LED zaświeca się na zielono, odcisk palca jest zapisany.
- Jeśli odcisk palca nie zostanie prawidłowo odczytany, rozlegną się 3 sygnały dźwiękowe, a pierścień LED zacznie migać na czerwono. To samo stanie się w przypadku próby wczytania już zapisanego odcisku palca.
- Jeżeli chcesz zaprogramować kolejny odcisk palca użytkownika, zacznij ponownie od wprowadzenia numeru miejsca w pamięci, patrz wyżej.
- Wyjdź z trybu parowania przyciskiem [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.17 Usuwanie odcisku palca użytkownika

Gdy tylko odpowiedni odcisk palca użytkownika zostanie usunięty, dany użytkownik nie będzie już mieć dostępu.

Przy usuwaniu odcisku palca użytkownika można postępować na dwa różne sposoby:

- Usunięcie odcisku palca użytkownika poprzez odczyt
- Usunięcie miejsce w pamięci, pod którym zapisany jest odcisk palca użytkownika.

12.17.1 Usunięcie odcisku palca użytkownika za pomocą odcisku palca

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.
- Wprowadź kod programowania [2], aby uruchomić tryb usuwania. Następnie dioda LED zaświeci się na żółto.
→ Alternatywnie do tych czynności można przytrzymać transponder główny 2x przed powierzchnią odczytu – lub dotknąć czujnika linii papilarnych 2x głównym odciskiem palca (każdorazowo w ciągu 5 sekund). Obydwie metody aktywują trybu usuwania, dioda LED świeci się na żółto.
- Dotknij czujnika linii papilarnych palcem użytkownika, który ma zostać usunięty. Po rozpoznaniu odcisku palca system dostępowy wyemituje krótki sygnał dźwiękowy i nastąpi usunięcie odcisku palca.
→ Jeśli odcisk palca użytkownika jest nieznan y i/lub już usunięty, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED zamiga na czerwono.
- Jeśli chcesz usunąć kolejne odciski palca użytkownika, należy postępować w powyżej opisany sposób.
- Wyjdź z trybu usuwania przyciskiem [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.17.2 Usuwanie odcisku palca użytkownika za pomocą numeru miejsca w pamięci

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.
- Wprowadź kod programowania [2], aby uruchomić tryb usuwania. Następnie dioda LED zaświeci się na żółto.
→ Alternatywnie do tych czynności można przytrzymać transponder główny 2x przed powierzchnią odczytu – lub dotknąć czujnika linii papilarnych 2x głównym odciskiem palca (każdorazowo w ciągu 5 sekund). Obydwie metody aktywują trybu usuwania, dioda LED świeci się na żółto.
- Wprowadź numer miejsca w pamięci ([0] [9] [8]), który chcesz usunąć, i potwierdź wpis przyciskiem [#]. Numer miejsca w pamięci (z zapisanymi w nim danymi) jest usuwany.
Przykład: [6] [#] = usunięcie miejsca w pamięci 6
- W razie potrzeby można teraz usunąć kolejne numery miejsc w pamięci (wprowadź numer miejsca w pamięci i naciśnij przycisk [#] w celu potwierdzenia).
- Wyjdź z trybu usuwania przyciskiem [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.18 Usuwanie wszystkich miejsc w pamięci

→ Opcja ta usuwa wszystkie 1000 miejsc w pamięci.

Transponder główny oraz dokonane programowania (np. czas aktywacji styku przełącznego) zostają zachowane.

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.

- Wprowadź kod programowania [2], aby uruchomić tryb usuwania. Następnie dioda LED zaświeci się na żółto.

→ Alternatywnie do tych czynności można przytrzymać transponder główny 2x przed powierzchnią odczytu – lub dotknąć czujnika linii papilarnych 2x głównym odciskiem palca (każdorazowo w ciągu 5 sekund). Obydwie metody aktywują tryb usuwania, dioda LED świeci się na żółto.

- Wprowadź kod główny i potwierdź go przyciskiem [#]. Wszystkie 1000 miejsc w pamięci zostanie usunięte.
- Wyjdź z trybu usuwania przyciskiem [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.19 Ustawianie czasu aktywacji dla styku przełącznego

Ta funkcja umożliwia ustawienie czasu aktywacji styku przełącznego w zakresie od 1 do 99 sekund po uzyskaniu prawidłowego dostępu do systemu kontroli dostępu (ustawienie domyślne to 5 sekund).

Jeśli ustawione jest „0”, styk przełączny przechodzi w tryb „Toggle” (przełączania). Przy każdej ważnej próbie dostępu zestyk przełączny zmienia położenie przełączania. Można to wykorzystać na przykład do uzbrajania/rozbrajania systemu alarmowego.

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.

- Wprowadź kod programowania [3] do ustawienia czasu aktywacji. Następnie dioda LED zaświeci się na żółto.

- Wprowadź żądany czas, na który styk przełączny ma być aktywowany. Możliwe jest [1] [9] [9] (= 1–99 sekund; bez zera wiodącego w przypadku jednocyfrowych numerów miejsc w pamięci).

Przykład 1: Czas aktywacji wynosi 8 sekund: [8]

Przykład 2: Tryb Toogle (przełączania): [0]

- Wyjdź z trybu ustawień za pomocą przycisku [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.20 Aktywacja lub dezaktywacja zabezpieczenia przed błędnymi wpisami

Ta funkcja umożliwia ustawienie, czy system kontroli dostępu ma być blokowany w przypadku dokonania 10 lub więcej nieprawidłowych wpisów z rzędu (ustawienie domyślne: wyłączone).

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.
- Wprowadź kod programowania [6] dla zabezpieczenia przed błędnymi wpisami. Następnie dioda LED zaświeci się na żółto.
- Wybierz żądaną funkcję:
 - 0 = funkcja zabezpieczenia jest wyłączona (ustawienie domyślne)
 - 1 = 10-minutowa blokada (w tym czasie nie jest możliwy dostęp do systemu za pomocą ważnego kodu PIN/ transpondera/ odcisku palca lub za pomocą klawiatury; główny transponder i główny odcisk palca nie działają; styk przełączny można aktywować przyciskiem automatu do otwierania drzwi); 10-minutową blokadę można zakończyć przedwcześnie poprzez krótkie odłączenie systemu kontroli dostępu.
 - 2 = blokada z alarmem na 1 do 3 minut (czas trwania alarmu można ustawić, jak opisano w [„12.21 Ustawianie czasu trwania alarmu dla funkcji zabezpieczenia” na stronie 35](#)); blokadę i alarm można zakończyć przedwcześnie za pomocą ważnego kodu PIN/ transpondera/ odcisku palca.



Ostrożnie!

Czas trwania sygnałów dźwiękowych jest regulowany w wielu krajach określonymi przepisami. Nawet jeśli sygnał dźwiękowy systemu kontroli dostępu nie jest tak głośny jak syrena instalacji alarmowej, może on nadal podlegać przepisom obowiązującym w danym kraju.

- Wyjdź z trybu ustawień za pomocą przycisku [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.21 Ustawianie czasu trwania alarmu dla funkcji zabezpieczenia

W przypadku aktywnej funkcji [2] (blokada z alarmem), jak opisano w [„12.20 Aktywacja lub dezaktywacja zabezpieczenia przed błędnymi wpisami” na stronie 35](#), czas trwania alarmu można ustawić, jak opisano poniżej (od 1 do 3 minut, ustawienie domyślne: 1 minuta).

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.
- Wprowadź kod programowania [5] dla ustawienia czasu trwania alarmu. Następnie dioda LED zaświeci się na żółto.
- Wprowadź żądany czas trwania alarmu. Możliwe jest [1] [3] (= 1–3 minuty).
- Wyjdź z trybu ustawień za pomocą przycisku [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.22 Aktywacja dostępu dla gości

System kontroli dostępu może zapisywać do 10 różnych transponderów lub kodów PIN gości. Dostępne są dla nich numery miejsce w pamięci 990–999.

Transpondery gości i kody PIN gości mogą mieć zaprogramowaną liczbę prób dostępu (od 1 do 10 prób), które stają się nieważne po ich wygaśnięciu. W ten sposób można na przykład zaprogramować transponder gościa, tak aby przyznawał dostęp tylko raz. Transponder gościa traci wtedy ważność.



Po wykorzystaniu zaprogramowanej liczby prób dostępu dla transpondera/PINu gościa system dostępu automatycznie usuwa transponder/PIN z pamięci. Do usuniętego numeru miejsca w pamięci można teraz przypisać nowy transponder/PIN gościa.

Zalecamy utworzenie tabeli i dokładne zapisanie wszystkich danych dostępowych (np. nazwisko gościa, liczba prób dostępu, numer miejsca w pamięci, numer transpondera i PIN). W przypadku transponderów gości należy również stosować transpondery o innym kolorze lub kształcie.

12.22.1 Programowanie transpondera gościa

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.
- Wprowadź kod programowania [1], aby rozpocząć proces programowania. Następnie dioda LED zaświeci się na żółto.

→ Alternatywnie do tych czynności można przytrzymać transponder główny 1x przed powierzchnią odczytu – lub dotknąć czujnika linii papilarnych 1x głównym odciskiem palca. Obydwie metody aktywują tryb zapisywania, dioda LED świeci się na żółto.

- Wprowadź numer miejsca w pamięci ([9] [9] [0] [9] [9] [9]), pod którym ma być zapisany transponder gościa i potwierdź numer miejsca w pamięci przyciskiem [#].

Przykład: [9] [9] [5] [#] = zapis transpondera gościa pod numerem miejsca w pamięci 995

→ Jeśli dany numer miejsca w pamięci jest już zajęty, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED będzie migać na czerwono. Nadpisanie miejsca w pamięci jest tym samym niemożliwe. Najpierw należy usunąć dany numer miejsca w pamięci, zanim będzie można zapisać pod nim transponder gościa.

- Wprowadź liczbę, ile razy może być użyty transponder gościa ([0] do [9], gdzie „0” oznacza 10-krotne użycie.).

Przykład 1: [2] = gość może użyć transpondera 2 razy, następnie traci on ważność

Przykład 2: [0] = gość może użyć transpondera 10 razy, następnie traci on ważność

- Potwierdź liczbę przyciskiem [#].
- Przytrzymaj transponder przed czujnikiem RFID. Po rozpoznaniu nowego transpondera system kontroli dostępu wyemituje krótki sygnał dźwiękowy i nastąpi zapis transpondera.

Zamiast trzymać transponder przed czujnikiem RFID można wprowadzić 8- lub 10-cyfrowy numer transpondera i potwierdzić przyciskiem [#].

Przykład: [0] [0] [0] [3] [1] [7] [1] [4] [5] [6] [#]

→ Jeśli parowanie transpondera jest już ukończone, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED będzie migać na czerwono. Tym samym wielokrotne parowanie tego samego transpondera nie jest możliwe.

- Jeżeli chcesz zaprogramować kolejny transponder gościa, zacznij ponownie od wprowadzenia numeru miejsca w pamięci, patrz wyżej.
- Wyjdź z trybu parowania przyciskiem [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [✖].

12.22.2 Zapisywanie PINu gościa

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.

- Wprowadź kod programowania [1], aby rozpocząć proces programowania. Następnie dioda LED zaświeci się na żółto.

→ Alternatywnie do tych czynności można przytrzymać transponder główny 1x przed powierzchnią odczytu – lub dotknąć czujnika linii papilarnych 1x głównym odciskiem palca. Obydwie metody aktywują tryb zapisywania, dioda LED świeci się na żółto.

- Wprowadź numer miejsca w pamięci ([9] [9] [0] [9] [9] [9]), pod którym ma być zapisany PIN gościa i potwierdź numer miejsca w pamięci przyciskiem [#].

Przykład: [9] [9] [5] [#] = zapis PINu gościa pod numerem miejsca w pamięci 995

→ Jeśli dany numer miejsca w pamięci jest już zajęty, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED będzie migać na czerwono. Nadpisanie miejsca w pamięci jest tym samym niemożliwe.

- Wprowadź liczbę, ile razy może być użyty PIN gościa ([0] [9], gdzie „0” oznacza 10-krotne użycie).

Przykład 1: [2] = gość może użyć PINu 2 razy, następnie traci on ważność

Przykład 2: [0] = gość może użyć PINu 10 razy, następnie traci on ważność

- Potwierdź liczbę przyciskiem [#].

- Teraz wprowadź żądany PIN gościa i potwierdź wpis przyciskiem [#].

Przykład: [2] [2] [2] [2] [#] = zapis PINu gościa 2222

→ PIN gościa może być 4–... 6-cyfrowy. Jednak kombinacja liczb 8888 nie jest możliwa, ponieważ jest to kombinacja serwisowa (standardowy kod użytkownika).

Jeśli dany PIN znajduje się już w jednym z miejsc w pamięci, system kontroli dostępu wyemituje 3 krótkie sygnały dźwiękowe, a dioda LED będzie migać na czerwono. Ten sam kod PIN można nadać tylko raz.

- Można zapisać kolejne kody PIN gości w sposób opisany powyżej, zaczynając od wprowadzenia numeru miejsca w pamięci.
- Wyjdź z trybu zapisywania przyciskiem [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.22.3 Usuwanie transpondera gościa lub PINu gościa

Transponder gościa lub PIN gościa jest automatycznie usuwany z pamięci po ustawionej liczbie prób dostępu.

Jeśli chcesz usunąć transponder gościa lub PIN gościa przed wykorzystaniem wszystkich prób dostępu, postępuj w taki sam sposób, jak w przypadku usuwania transpondera użytkownika lub kodu PIN użytkownika; po prostu wprowadź odpowiedni numer miejsca w pamięci ([9] [9] [0] [9] [9] [9]) dla gościa.

- Informacje na temat usuwania transpondera można znaleźć w rozdziale [„12.15 Usuwanie transpondera użytkownika” na stronie 30](#).
- Informacje na temat usuwania kodu PIN można znaleźć w rozdziale [„12.13 Usuwanie PINu użytkownika” na stronie 26](#).

12.23 Dodawanie użytkowników antynapadowych

Użytkownicy antynapadowi mogą uruchomić dodatkowy alarm bezpieczeństwa, aby poinformować personel ochrony o incydencie związanym z bezpieczeństwem. Do skonfigurowania użytkownika antynapadowego wymagany jest dodatkowy alarm. Łącznie można zarejestrować dwóch (2 x) użytkowników antynapadowych.

Wymaganie

- ID (identyfikator) użytkownika: 988, 989

Rejestrowanie transpondera

Kroki	Kombinacja przycisków/obsługa
1. Aktywacja trybu programowania	[*] (kod główny) [#]
2. Zarejestruj transponder.	Korzystanie z karty: [1] (ID (identyfikator) użytkownika) [#] (odczyt karty) [#] Korzystanie z numeru karty: [1] (ID (identyfikator) użytkownika) [#] (8-/10-/17-cyfrowy numer karty) [#]
3. Wyjście z trybu programowania	[*]

Rejestrowanie kodu PIN

Kroki	Kombinacja przycisków/obsługa
1. Aktywacja trybu programowania	[*] (kod główny) [#]
2. Zarejestruj PIN.	Długość PINu: 4–6 cyfr (poza 8888) [1] (ID (identyfikator) użytkownika) [#] (PIN) [#]
3. Wyjście z trybu programowania	[*]

Usuwanie transponderów antynapadowych i kodów PIN

- Informacje na temat usuwania transpondera można znaleźć w rozdziale „[12.15 Usuwanie transpondera użytkownika](#)” na stronie 30.
- Informacje na temat usuwania kodu PIN można znaleźć w rozdziale „[12.13 Usuwanie PINu użytkownika](#)” na stronie 26.

12.24 Aktywacja/dezaktywacja wskazania optycznego i akustycznego

Komunikat o działaniu i komunikat o błędach systemu kontroli dostępu towarzyszą wskazania LED i sygnały dźwiękowe. Oba te elementy można aktywować i dezaktywować (ustawienie domyślne: wskazania LED i sygnały dźwiękowe są aktywowane).

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.
- Wprowadź kod programowania [7] do ustawienia wskazań LED i sygnałów dźwiękowych. Następnie dioda LED zaświeci się na żółto.
- Wybierz żądaną funkcję:
 - [0] = sygnały dźwiękowe wyłączone
 - [1] = sygnały dźwiękowe włączone (ustawienie domyślne)
 - [2] = dioda LED wyłączona
 - [3] = dioda LED włączona (ustawienie domyślne)
 - [4] = podświetlenie przycisków wyłączone
 - [5] = podświetlenie przycisków włączone
 - [6] = podświetlenie przycisków aktywuje się po naciśnięciu przycisku (pierwsze naciśnięcie przycisku aktywuje jedynie podświetlenie przycisków); podświetlenie przycisków jest automatycznie wyłączane, jeśli żaden przycisk nie zostanie naciśnięty w ciągu 20 sekund (ustawienie fabryczne).
- Wyjdź z trybu ustawień za pomocą przycisku [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].

12.25 Aktywacja sieci WLAN

- Podłącz system kontroli dostępu do zasilania, aby aktywować sieć WLAN.

12.26 Transmisja danych pomiędzy dwoma systemami kontroli dostępu

Jeśli używane są dwa identyczne systemy kontroli dostępu, dane transponderów i kodów PIN mogą być wymieniane między urządzeniami.

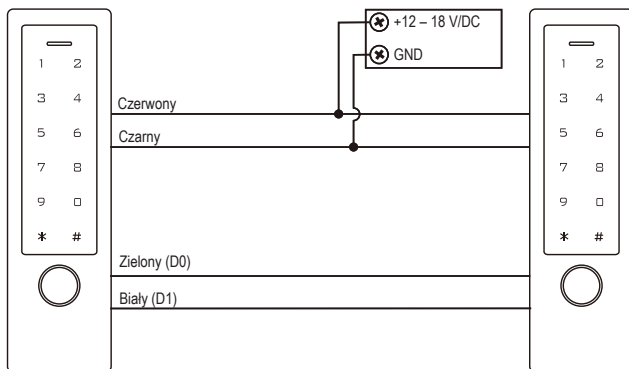
→ Uwaga:

Transmisja danych odcisków palców nie jest możliwa.

Kod główny obu systemów kontroli dostępu musi być taki sam.

Należy postępować w następujący sposób:

- Podłącz dwa identyczne systemy kontroli dostępu w następujący sposób:



- Włącz zasilanie.

→ Uwaga:

Poniższe wpisy należy wprowadzać wyłącznie w urządzeniu, którego dane (transpondery/PINy) mają zostać przesyłane.

Na urządzeniu docelowym (które ma odbierać dane) nie należy nic wpisywać.

- Wywołaj tryb programowania w systemie kontroli dostępu, którego dane transponderów lub kodów PIN chcesz przesyłać, zgodnie z opisem w rozdziale [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED miga na czerwono.
- Wprowadź kod programowania [9][8] i naciśnij przycisk [#], aby rozpocząć transmisję danych. Dioda LED świeci się na zielono; transmisja może trwać do ok. 30 sekund. Następnie system kontroli dostępu wyemituje sygnał dźwiękowy, a dioda LED zaświeci się na czerwono.
- Wyjdź z trybu programowania przyciskiem [*].
- Odłącz oba systemy kontroli dostępu od zasilania. Następnie można zainstalować i okablować urządzenia w standardowy sposób, a następnie przeprowadzić dalsze programowanie w obu systemach kontroli dostępu oddzielnie (np. czas aktywacji styku przelącznego).

12.27 Ustawianie formatu wejściowego danych Wiegand

Ta opcja jest wymagana, jeśli chcesz obsługiwać czytnik zewnętrzny za pośrednictwem złącza Wiegand systemu kontroli dostępu (system kontroli dostępu służy jako urządzenie nadrzędne (Master) lub sterownik Wiegand).

W instrukcji obsługi czytnika zewnętrznego należy przeczytać, jaki format danych wyjściowych generuje. Następnie należy odpowiednio dostosować ustawienia w systemie kontroli dostępu.

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.
 - Wprowadź kod programowania [8], aby uruchomić tryb ustawień. Następnie dioda LED zaświeci się na żółto.
 - Wprowadź teraz:
 - [2] [6] [4] [4] = szybkość przesyłania danych 26 do 44 bitów (ustawienie domyślne 26 bitów)
 - lub
 - [4] = format wejściowy PINu 4 bity (ustawienie domyślne)
 - lub
 - [8] = format wejściowy PINu 8 bitów
 - lub
 - [1] [0] = format wejściowy PINu 10 bitów
 - lub
 - [0] = bit parzystości dezaktywowany
 - lub
 - [1] = bit parzystości aktywowany (ustawienie domyślne)
 - Wyjdź z trybu ustawień za pomocą przycisku [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].
- W przypadku czytników o szybkości przesyłania danych 32 lub 40 bitów bit parzystości musi być dezaktywowany.

12.28 Ustawianie formatu wyjściowego danych Wiegand

Ta opcja jest wymagana, jeśli system kontroli dostępu ma działać jako czytnik na sterowniku Wiegand.

Można ustawić zarówno szybkość przesyłania danych, jak i aktywować/dezaktywować bit parzystości. Odnośnie formatu danych należy przestrzegać instrukcji obsługi sterownika Wiegand. Następnie należy ustawić taką samą szybkość przesyłania danych w systemie kontroli dostępu i odpowiednio aktywować/dezaktywować bit parzystości.

- Aktywuj tryb programowania zgodnie z opisem w [„12.4 Aktywacja/dezaktywacja trybu programowania” na stronie 18](#); dioda LED zacznie migać na czerwono.
 - Wprowadź kod programowania [8], aby uruchomić tryb ustawień. Następnie dioda LED zaświeci się na żółto.
 - Wprowadź teraz:
 - [2] [6] [4] [4] = szybkość przesyłania danych 26 do 44 bitów (ustawienie domyślne 26 bitów)
 - lub
 - [4] = format wyjściowy PINu 4 bity (ustawienie domyślne)
 - lub
 - [8] = format wyjściowy PINu 8 bitów
 - lub
 - [1] [0] = format wyjściowy PINu 10 bitów
 - lub
 - [0] = bit parzystości dezaktywowany
 - lub
 - [1] = bit parzystości aktywowany (ustawienie domyślne)
 - Wyjdź z trybu ustawień za pomocą przycisku [#]. Dioda LED będzie ponownie migać na czerwono, można teraz dokonać dalszego programowania lub wyjść z trybu programowania przyciskiem [*].
- W przypadku złącza sterownika Wiegand o szybkości przesyłania danych 32 lub 40 bitów bit parzystości musi być dezaktywowany.

13 Obsługa

13.1 Dostęp za pomocą ważnego PINu/ transpondera/ odcisku palca użytkownika

Po rozpoznaniu przez system kontroli dostępu ważnego PINu użytkownika, transpondera użytkownika lub odcisku palca użytkownika styk przełączny (i np. sterowany przez niego zamek drzwi) zostanie aktywowany na ustawiony czas, dioda LED świeci się na zielono. Po upływie tego czasu dioda LED zaświeci się na czerwono (tryb gotowości).

→ Jeśli użytkownik musi wprowadzić więcej niż jedno poświadczenie uprawnienia w celu uwierzytelnienia (np: transponder + PIN), użytkownik musi wprowadzić wszystkie poświadczenia uprawnienia w ciągu 5 sekund. Po 5 sekundach system kontroli dostępu przechodzi w tryb gotowości. Dalsze informacje na ten temat można znaleźć w rozdziale [„12.11 Wybór trybu dostępu” na stronie 23](#).

13.2 Dostęp poprzez przycisk automatu do otwierania drzwi

Krótkie naciśnięcie przycisku automatu do otwierania drzwi aktywuje styk przełączny i sterowany przez niego automat do otwierania drzwi na ustawiony czas, dioda LED świeci się na zielono.

13.3 Zapobieganie odczytaniu PINu

Jako funkcję specjalną podczas wprowadzania kodu PIN można wprowadzić dodatkowe cyfry przed lub po właściwym PINie. Można wprowadzić do 10 cyfr, w których można „ukryć” rzeczywisty kod PIN.

→ **Uwaga:**

Ta opcja jest dostępna tylko wtedy, gdy używasz 6-cyfrowych kodów PIN.

Przykład: PIN użytkownika = 1 2 1 2 1 2

Wprowadź: 9 9 9 1 2 1 2 1 2 9 #

→ Nie ma znaczenia, czy i ile cyfr wpiszesz przed i/lub po właściwym PINie. W sumie może to być maksymalnie 10 cyfr, w których musi być zawarty prawidłowy PIN.

13.4 Dezaktywacja alarmu/blokady w przypadku nieprawidłowego wpisu

Jeśli zabezpieczenie przed nieprawidłowymi wpisami jest aktywne, system kontroli dostępu emituje sygnał alarmowy przez ustawiony czas, a dioda LED miga na czerwono.

Alarm może zostać zakończony poprzez ważną próbę dostępu (ważny PIN użytkownika, transponder użytkownika lub odcisk palca użytkownika) lub transponder główny albo główny odcisk palca.

→ **Uwaga:**

Jeśli funkcja 10-minutowej blokady 1 jest aktywna, można ją przedwcześnie zakończyć poprzez krótkie odłączenie systemu kontroli dostępu od zasilania.

Więcej informacji na ten temat można znaleźć w rozdziale [„12.20 Aktywacja lub dezaktywacja zabezpieczenia przed błędnymi wpisami” na stronie 35](#) dotyczącym szczegółów konfiguracji.

14 Rozwiązywanie problemów

Po awarii zasilania system kontroli dostępu zachowuje swoje ustawienia i jest natychmiast gotowy do ponownego działania. Jednakże podczas awarii zasilania system kontroli dostępu nie funkcjonuje.

→ W zależności od przeznaczenia – ze względów bezpieczeństwa – zalecamy, aby system kontroli dostępu (podobnie jak w przypadku instalacji alarmowej) był zasilany za pomocą zasilania bezprzewodowego.

Automat do otwierania drzwi nie działa

- Styk przełączny jest bezpotencjałowy. Oznacza to, że trzeba wykonać odpowiednie zewnętrzne okablowanie, ponieważ system kontroli dostępu nie zasila automatu do otwierania drzwi.
- Jeśli automat do otwierania drzwi posiada odpowiednie oznaczenie biegunowości (plus/+ i minus/-), zwróć uwagę na prawidłowe podłączenie do systemu kontroli dostępu i zasilania.
- Sprawdź biegunowość diody ochronnej podłączonej do automatu do otwierania drzwi.
- Używany transponder lub odcisk palca nie jest zaprogramowany, wprowadzony PIN jest niezany.
- Styk przełączny nie może zostać aktywowany za pomocą głównego transpondera lub głównego odcisku palca.
- Zestyki NO/NC powinny być prawidłowo okablowane w zależności od zastosowanego automatu do otwierania drzwi (automat do otwierania drzwi Fail-Safe lub Fail-Secure).

Zapisywanie nowego PINu użytkownika nie działa

- Nie można użyć kombinacji numerów 8888, ponieważ jest to domyślne ustawienie dla pamięci wewnętrznej w trybie dostępu „PIN + transponder”.
- PIN użytkownika jest już używany. Dwukrotne zapisanie tego samego PINu nie jest możliwe.

Transponder nie został rozpoznany

- Zawsze trzymaj tylko jeden transponder przed czujnikiem RFID.
- Upewnij się, że transponder znajduje się wystarczająco blisko systemu kontroli dostępu (ok. 2 cm).
- Można używać wyłącznie transponderów EM o częstotliwości 125 kHz.
- Metalowe przedmioty mogą zakłócać działanie transpondera (np. jeśli transponder znajduje się w portfelu z monetami).

Programowanie nowego transpondera użytkownika nie funkcjonuje

- Zawsze trzymaj tylko jeden transponder przed czujnikiem RFID.
- Upewnij się, że transponder znajduje się wystarczająco blisko systemu kontroli dostępu (ok. 2 cm).
- Można używać wyłącznie transponderów EM o częstotliwości 125 kHz.
- Miejsce w pamięci jest już zajęte. Użyj innego miejsca w pamięci lub usuń istniejące, zanim będzie można w nim zaprogramować inny transponder.
- Jeśli sterownik Wiegand korzysta z czytnika kart dla transponderów 125 kHz, programowanie można przeprowadzić zarówno za pośrednictwem systemu kontroli dostępu, jak i zewnętrznego czytnika kart. Użyj zewnętrznego czytnika kart, aby sprawdzić działanie.

Programowanie odcisków palca użytkowników nie działa lub działa nieprawidłowo

- W razie potrzeby użyj testowo innego palca. Aby odcisk palca był ważny, czujnik linii papilarnych musi wykryć wystarczającą liczbę linii papilarnych (wypukłości).
- Przyłóż palec na środku całej jego powierzchni. Wykryty obszar powierzchni skóry musi mieć minimalną wielkość, aby był ważny. Jednak orientacja palca nie ma znaczenia. Można więc w każdej chwili zaprogramować palec „pionowo”, a później przyłożyć go obróconego o 90° w celu uzyskania dostępu.
- Nie noś rękawic.
- Czujnik linii papilarnych należy czyścić przy użyciu czystej, miękkiej i suchej szmatki.

Styk przełączny jest stale aktywny (i nie przełącza się z powrotem).

- Czas aktywacji styku przełącznego został ustawiony na „0” i znajduje się on w trybie Toggle (przełączania). Przy każdej ważnej próbie dostępu zestyk przełączny zmienia położenie przełączania.

Styk przełączny nie może zostać aktywowany za pomocą prawidłowo zaprogramowanego kodu PIN użytkownika, transpondera użytkownika lub odcisku palca użytkownika.

- Sprawdzić ustawienie trybu dostępu. Dalsze informacje na ten temat można znaleźć w rozdziale [„12.11 Wybór trybu dostępu” na stronie 23](#).

Po przywróceniu ustawień fabrycznych kody PIN użytkownika, transpondery użytkownika, odciski palców użytkownika oraz główny odcisk palca nie są usunięte.

- Jest to normalne zjawisko.

PIN gościa lub transponder gościa nie działa

- Kod PIN gościa lub transponder gościa jest ważny tylko przez określoną liczbę prób dostępu. Kod PIN gościa lub transponder gościa jest następnie automatycznie unieważniany i usuwany z pamięci systemu kontroli dostępu.
- Można ponownie przywrócić ważność używanego transpondera i przekazać go innemu gościowi, przeprogramowując go za pośrednictwem systemu kontroli dostępu i nadając określoną liczbę prób dostępu.

Złącze Wiegand nie działa

- Zwróć uwagę na to, aby nie zamienić obu przewodów danych D0 i D1; D0 musi być zawsze podłączone do D0, a D1 do D1.
- Zaprogramuj złącze Wiegand. Szczegółowe informacje na ten temat zawierają rozdziały [„12.27 Ustawianie formatu wejściowego danych Wiegand” na stronie 41](#) i [„12.28 Ustawianie formatu wyjściowego danych Wiegand” na stronie 42](#).
- W każdym przypadku należy przestrzegać instrukcji obsługi urządzenia, które ma zostać podłączone do złącza Wiegand.

15 Deklaracja zgodności (DOC)

My, Conrad Electronic SE, Klaus-Conrad-Straße 1, D-92240 Hirschau, deklarujemy, że produkt ten jest zgodny z postanowieniami Dyrektywy 2014/53/UE.

Pełny tekst deklaracji zgodności UE jest dostępny pod następującym adresem internetowym:

www.conrad.com/downloads

Wybierz język, klikając na symbol flagi i wprowadź numer katalogowy produktu w polu wyszukiwania; następnie możesz pobrać deklarację zgodności UE w formacie pdf.

16 Konserwacja i czyszczenie

Ten produkt nie wymaga konserwacji. Do okazjonalnego czyszczenia używaj suchej, niestrzępiącej się szmatki. W przypadku silnych zabrudzeń szmatkę można zwilżyć wodą.

W żadnym wypadku nie stosuj agresywnych środków czyszczących, alkoholu lub innych roztworów chemicznych, ponieważ mogą one spowodować odbarwienie lub uszkodzenie.

17 Utylizacja



Wszystkie urządzenia elektryczne i elektroniczne wprowadzane na rynek europejski muszą być oznaczone tym symbolem. Ten symbol oznacza, że po zakończeniu okresu użytkowania urządzenie to należy usunąć utylizować oddzielnie od niesortowanych odpadów komunalnych.

Każdy posiadacz zużytego sprzętu jest zobowiązany do przekazania zużytego sprzętu do selektywnego punktu zbiórki odrębnie od niesegregowanych odpadów komunalnych. Przed przekazaniem zużytego sprzętu do punktu zbiórki użytkownicy końcowi są zobowiązani do wyjęcia zużytych baterii i akumulatorów, które nie są zabudowane w zużytym sprzęcie, a także lamp, które można wyjąć ze zużytego sprzętu, nie niszcząc ich.

Dystrybutorzy urządzeń elektrycznych i elektronicznych są prawnie zobowiązani do nieodpłatnego odbioru zużytego sprzętu. Conrad oferuje następujące **możliwości bezpłatnego zwrotu** (więcej informacji na naszej stronie internetowej):

- w naszych filiach Conrad
- w punktach zbiórki utworzonych przez Conrad
- w punktach zbiórki publiczno-prawnych zakładów utylizacji lub w systemach zbiórki utworzonych przez producentów i dystrybutorów w rozumieniu ElektroG (niemiecki system postępowania ze złomem elektrycznym i elektronicznym).

Użytkownik końcowy jest odpowiedzialny za usunięcie danych osobowych ze zużytego sprzętu przeznaczonego do utylizacji.

Należy pamiętać, że w krajach poza Niemcami mogą obowiązywać inne obowiązki dotyczące zwrotu i recyklingu zużytego sprzętu.

18 Dane techniczne

18.1 Oprogramowanie

Aplikacja mobilna.....Tuya Smart Life – Smart Living

18.2 Zasilanie

Zasilanie12–18 V/DC

Pobór prądu.....w trybie czuwania <= 60 mA; maks. <= 150 mA

18.3 Dostęp

Złącze Wiegand.....Tak; 26–44 bity Wejście i wyjście

Odpowiednie transpondery.....Dostępne na rynku transpondery EM dla częstotliwości 125 kHz

Zachowanie danych w razie awarii

zasilania.....Tak

Odległość odczytu kartymaks. 3 cm

Zakres częstotliwości karty.....124,6–125,4 kHz

Moc nadawcza karty.....11,62 dBm

Miejsca w pamięci na transpondery/

kody PIN1000 (988 użytkowników wspólnych, 2 użytkowników antynapadowych,
10 użytkowników-gości)

Miejsca w pamięci na odciski palców100 (w tym 99 odcisków palca użytkownika i 1 główny odcisk palca)

Częstotliwość WLAN2,4 GHz

Standard WLAN.....IEEE 802.11b/g/n

Zakres częstotliwości WLAN2412–2472 MHz

Moc nadawcza WLAN16,39 dBm

Zasięg WLANmaks. 25 m (w otwartym terenie)

18.4 Wyjście

Typ.....Bezpotencjałowy jednobiegunowy zestaw przełączny (przełącznik)

Maks. moc załączalna24 V/DC, 2 A

Regulowany czas przełączania1–99 sekund lub tryb przełączania (toggle); ustawienie domyślne:
5 sekund

18.5 Otoczenie

Miejsce montażu.....Wewnątrz/na zewnątrz

Stopień ochrony.....IP66

Warunki otoczeniaTemperatura od -30°C do +60°C

18.6 Inne

Materiał.....Stop cynku

Długość kablaok. 90 cm

Wymiary (szer. x wys. x głęb.)166 x 45 x 22 mm

Wagaok. 387 g

 To publikacja została opublikowana przez Conrad Electronic SE, Klaus-Conrad-Str. 1, D-92242 Hirschau, Niemcy (www.conrad.com).

Wszelkie prawa odnośnie tego tłumaczenia są zastrzeżone. Reprodukowanie w jakiegokolwiek formie, kopiowanie, tworzenie mikrofilmów lub przechowywanie za pomocą urządzeń elektronicznych do przetwarzania danych jest zabronione bez pisemnej zgody wydawcy. Powielanie w całości lub w części jest zabronione. Publikacja ta odpowiada stanowi technicznemu urządzeń w chwili druku.

Copyright 2024 by Conrad Electronic SE.