Roger Access Control System

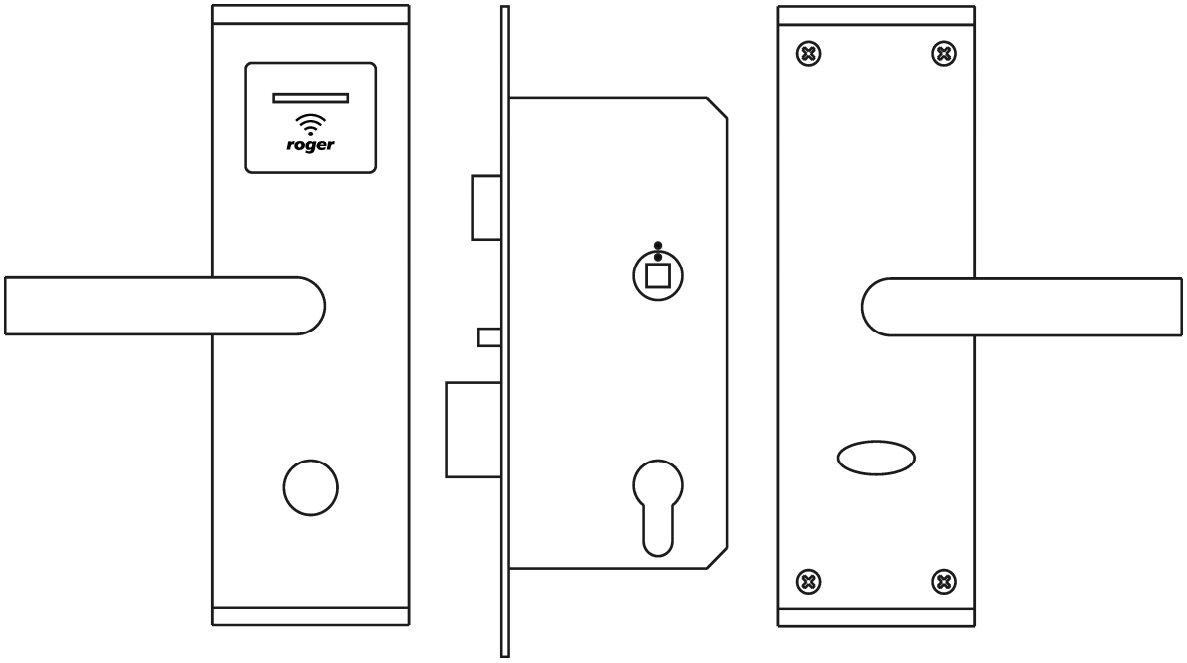
Zamek bezprzewodowy RWL-1 v1.0

Instrukcja obsługi

Oprogramowanie wbudowane: 1.1

Wersja dokumentu: Rev. D

CE



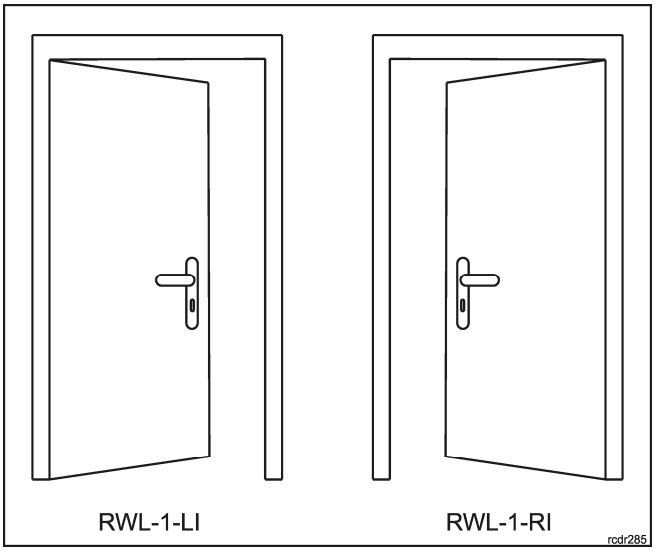
BUDOWA I PRZEZNACZENIE

Zamek RWL-1 umożliwia jednostronną elektroniczną kontrolę dostępu do pomieszczenia przy użyciu kart zbliżeniowych standardu MIFARE. Zamek RWL-1 może pracować w *Trybie sieciowym* w ramach systemu kontroli dostępu i automatyki budynkowej RACS 5 lub w *Trybie autonomicznym*. W *Trybie sieciowym*, decyzje o przyznaniu dostępu są podejmowane w zewnętrznym kontrolerze dostępu, z którym zamek jest połączony bezprzewodowo. W *Trybie autonomicznym*, dostęp przyznawany jest w oparciu o listę kart zbliżeniowych przechowywanych w wewnętrznej pamięci zamka. W przypadku awarii połączenia radiowego lub utraty łączności z kontrolerem, zamek automatycznie przechodzi z *Trybu sieciowego* do *Trybu autonomicznego* i kontynuuje kontrolę dostępu w oparciu o dane przechowywane w swojej pamięci.

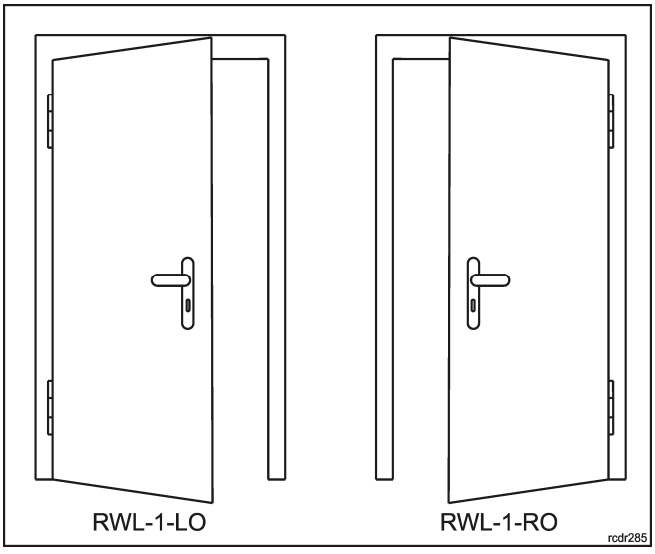
Zamek składa się z dwóch szyldów zespolonych z klamkami oraz zamka wpuszczanego w skrzydło. Czytnik kart jest umieszczony w szyldzie zewnętrznym natomiast pojemnik na baterie, w szyldzie wewnętrznym. Rygiel zamka jest na stałe sprzęgnięty z klamką wewnętrzną, co powoduje, że drzwi mogą być otwarte w dowolnej chwili od wewnątrz bez użycia karty i przy braku zasilania bateryjnego. Klamka zewnętrzna w stanie spoczynku jest odseparowana od rygla i porusza się swobodnie. W momencie przyznania dostępu układ elektroniczny sprzęga klamkę zewnętrzną z ryglem i zatrzaskiem, co umożliwia otwarcie drzwi od zewnątrz. W momencie zamknięcia drzwi rygiel zamka jest samoczynnie zwalniany, co powoduje uzyskanie pełnego poziomu zabezpieczenia drzwi przed otwarciem. Zamek może być opcjonalnie wyposażony w wkładkę patentową, która umożliwia awaryjne otwarcie drzwi od zewnątrz przy pomocy tradycyjnego klucza mechanicznego. Zamek jest wyposażony w czujnik położenia rygla oraz czujnik położenia pokrętła znajdującego się na szyldzie wewnętrznym. Opcjonalnie, do zamka można podłączyć zewnętrzny czujnik otwarcia drzwi. Stany wszystkich czujników są raportowane do systemu kontroli dostępu. Zamek jest zasilany z 4 baterii AA. Niski stan baterii zasilających zamek może być sygnalizowany lokalnie oraz raportowany do kontrolera dostępu. Przy założeniu 10 odczytów dziennie, zestaw nowych baterii wystarcza na ok. 2 lata pracy zamka.

W zależności od tego czy drzwi otwierają się do wnętrza czy na zewnątrz, oraz od tego, czy klamka znajduje się po lewej czy po prawej stronie skrzydła, konieczne jest zastosowanie odpowiedniej, jednej z czterech odmian zamka.

Wersja	Opis
RWL-1-LI	Drzwi prawe otwierane do wnętrza
RWL-1-RI	Drzwi lewe otwierane do wnętrza
RWL-1-LO	Drzwi lewe otwierane na zewnątrz
RWL-1-RO	Drzwi prawe otwierane na zewnątrz



Rys. 1. Zastosowanie zamka RWL-1 w drzwiach otwieranych do wnętrza (widok od strony korytarza)

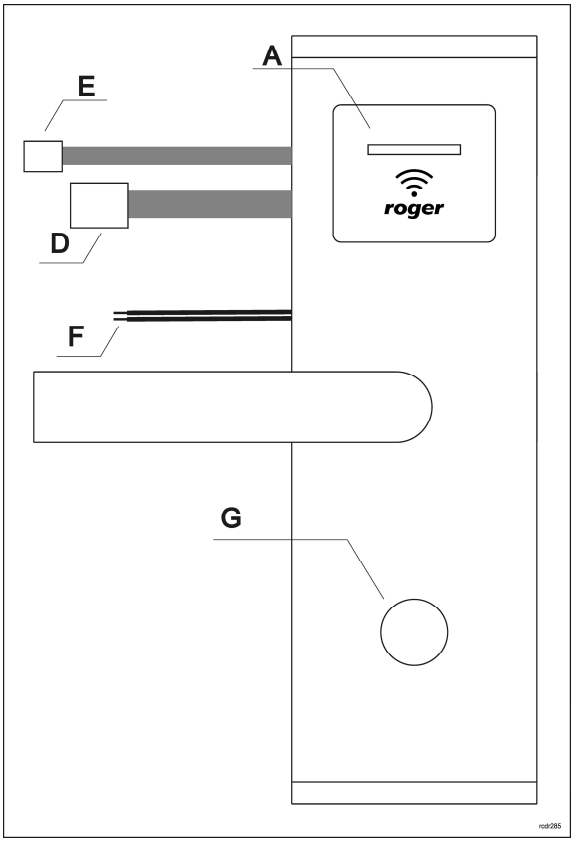


Rys. 2. Zastosowanie zamka RWL-1 w drzwiach otwieranych na zewnątrz (widok od strony korytarza)

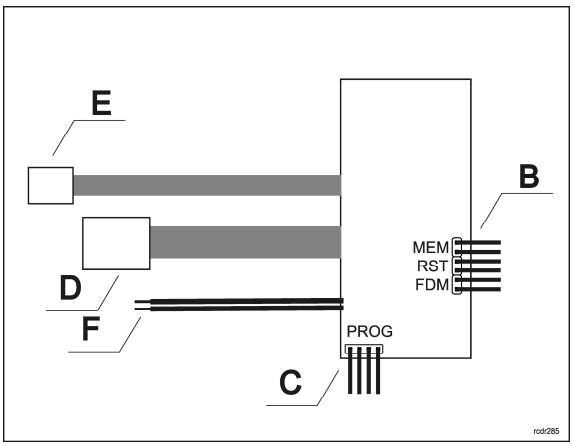
Konstrukcja mechaniczna

Okucie zewnętrzne

Okucie zewnętrzne składa się z szyldu zespolonego z klamką i montowanego od strony wejścia do kontrolowanego pomieszczenia. W szyldzie zewnętrznym umieszczony jest moduł elektroniczny czytnika kart zbliżeniowych (A) oraz otwór na połówkową wkładkę bębenkową (G) służącą do awaryjnego otwierania drzwi za pomocą klucza mechanicznego. Na module elektronicznym znajdującym się w szyldzie, umieszczone są kontakty serwisowe (B) oraz złącze (C) do podłączenia kabla programującego. Z modułu elektronicznego wychodzi wiązka przewodów zakończona większą wtyczką (D), która służy do połączenia z zamkiem wpuszczanym oraz mniejsza wtyczka (E), która służy do połączenia z koszykiem na baterie. Z modułu wychodzą dodatkowo, dwa przewody (F) zaizolowane na końcach koszulką termokurczliwą, które przeznaczone są do podłączenia zewnętrznego czujnika otwarcia drzwi. Stan tego czujnika jest reprezentowany w systemie kontroli dostępu, jako wejście DOOR CONTACT.



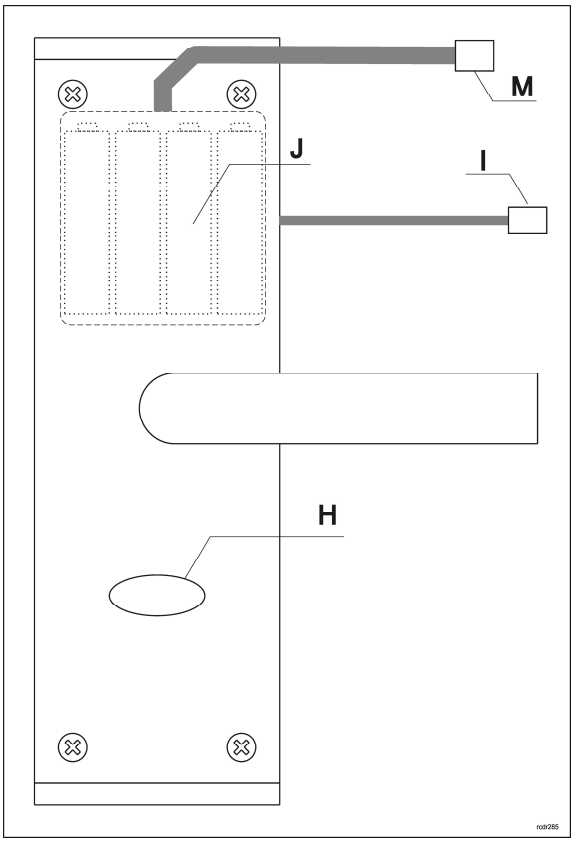
Rys. 3. Okucie zewnętrzne



Rys. 4. Moduł elektroniczny w szyldzie zewnętrznym

Okucie wewnętrzne

Okucie wewnętrzne składa się z szyldu zespolonego z klamką montowanego od strony wyjścia z pomieszczenia. Na szyldzie dostępne jest pokrętło (H). Z pokrętłem tym jest sprzężony czujnik, którego styki wyprowadzone są na konektorze (I). Konektor I należy połączyć z pasującym do niego gniazdkiem K znajdującym się na przewodach wychodzących z zamka wewnętrznego. W *Trybie sieciowym* stan pokrętła jest raportowany do kontrolera dostępu za pośrednictwem linii wejściowej KNOB SWITCH, której funkcja podlega programowaniu w programie zarządzającym systemem kontroli dostępu VISO. W *Trybie autonomicznym* przekręcenie pokrętła blokuje możliwość otwarcia drzwi przy pomocy kart zbliżeniowych. Naciśnięcie klamki powoduje automatyczny powrót pokrętła do pozycji spoczynkowej. W szyldzie wewnętrznym umieszczony jest koszyk na baterie (J). W celu wymiany baterii należy odkręcić dwie górne śruby mocujące okucie i wysunąć koszyk z bateriami. Z koszyka wychodzi wiązka przewodów zakończona wtykiem (M). Wtyk ten należy połączyć z pasującym do niego gniazdkiem E wychodzącym z modułu elektronicznego w szyldzie zewnętrznym.

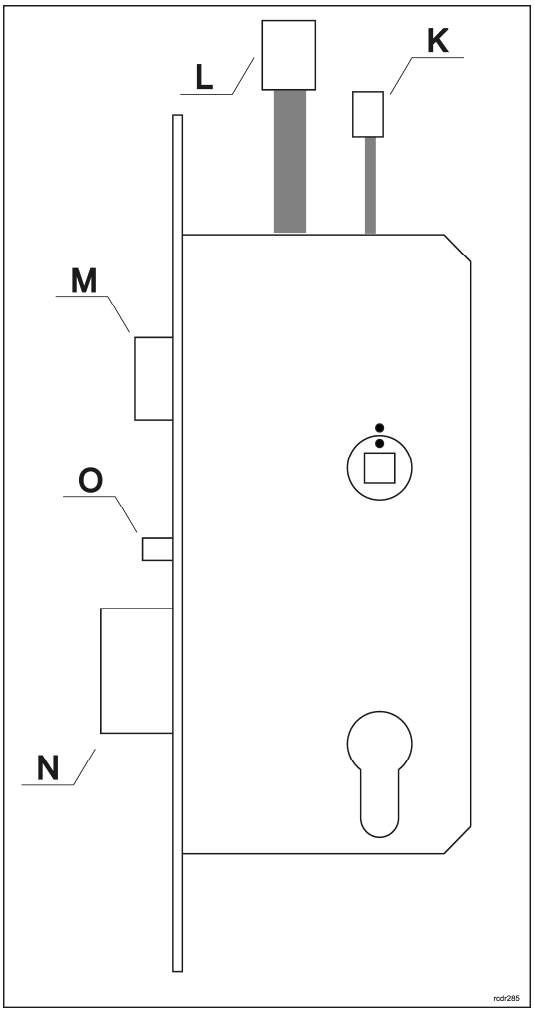


Rys. 5. Okucie wewnętrzne

Zamek wpuszczany

Zamek wewnętrzny zawiera serwomechanizm sterowany z poziomu modułu elektronicznego znajdującego się w szyldzie zewnętrznym. Z zamka wychodzą dwie wiązki przewodów zakończonych tzw. dużą wtyczką oraz małą wtyczką. Duża wtyczka (L) służy do połączenia z okuciem zewnętrznym natomiast mała wtyczka (K) z okuciem wewnętrznym.

Zamek jest wyposażony w zatrzask (M), rygiel (N) oraz bolec zwalniający (O). Zaryglowanie drzwi następuje automatycznie po zamknięciu skrzydła. Stan rygla jest raportowany do kontrolera dostępu (wejście: DEADBOLT CONTACT). Odryglowanie drzwi może nastąpić poprzez użycie klamki wewnętrznej, klamki zewnętrznej oraz za pomocą kluczyka wkładki bębenkowej. Odblokowanie rygla z poziomu klamki zewnętrznej może nastąpić jedynie po jej zasprzęgleniu przez serwomechanizm znajdującym się w zamku wpuszczanym. Chwilowe zasprzęglenie klamki następuje po przyznaniu dostępu. Gdy zamek pracuje w *Trybie biurowym* klamka zewnętrzna jest zasprzęglona na stałe. Zamek wpuszczany posiada rozstaw 72mm.



Rys. 6. Zamek wpuszczany

Wkładka mechaniczna

W zamku RWL-1 można zastosować tzw. połówkową wkładkę bębenkową. Wkładka ta umożliwia otwarcie awaryjne drzwi od zewnątrz przy pomocy klucza. Wielkość wkładki zależy od grubości drzwi i powinna być tak dobrana, aby nie wystawała więcej niż 12mm ponad powierzchnię drzwi. W komplecie z zamkiem dostarczana jest wkładka bębenkowa 26/10, którą można wykorzystać w skrzydłach o grubości od 38 do 55mm.

OPIS FUNKCJONALNY

Zamek może być wykorzystany, jako autonomiczny punkt kontroli dostępu, w którym dostęp jest przyznawany w oparciu o dane zapisane w wewnętrznej pamięci urządzenia lub jako element sieciowego systemu kontroli dostępu, w którym działanie zamka jest pod kontrolą zewnętrznego kontrolera dostępu. W *Trybie sieciowym* transmisja danych do kontrolera dostępu odbywa się droga radiową i wymaga pośrednictwa koncentratora RWH-1. Bez względu na docelowy tryb pracy zamka, wymaga on wcześniejszego skonfigurowania. Jeśli zamek ma pracować w *Trybie autonomicznym* to możliwe jest jego manualne skonfigurowanie bez użycia komputera.

Uwaga: Ze względu na małe wymiary breloków zbliżeniowych, mogą one nie być poprawnie wykrywane przez wbudowany czujnik zbliżeniowy. W zamkach serii RWL rekomendowane jest stosowanie pełnowymiarowych kart zbliżeniowych.

Identyfikatory zbliżeniowe

Zamek jest wyposażony w czytnik identyfikatorów zbliżeniowych pracujących w standardzie MIFARE® Ultralight/Classic/DESFire/Plus. Domyślnie, fabrycznie nowy czytnik skonfigurowany jest do odczytu numeru seryjnego karty (tzw. CSN – *Chip Serial Number*), niemniej za pomocą programu RogerVDM można przekonfigurować go do odczytu numeru zapisanego w programowalnych obszarach kart MIFARE® (tzw. PCN – *Programmable Card Number*).

Kod karty

Kod karty (RCN), odczytywany przez czytnik zamka powstaje przez złożenie dwóch numerów składowych (RCN=CSN+PCN):

- Sekcji CSN
- Sekcji PCN

Sekcja CSN to fragment kodu karty, który pobierany jest z seryjnego numeru karty (CSN). Numer CSN jest programowany w czasie produkcji karty.

Sekcja PCN to fragment kodu karty, który pobierany z programowalnych obszarów pamięci karty. Numer PCN może być zaszyfrowany indywidualnym kluczem i przez to być zabezpieczony przed kopiowaniem na inne karty.

Ze względu na łatwość powielania numeru seryjnego kart, zaleca się takie skonfigurowanie czytnika aby korzystał on z numeru zapisanego w szyfrowanych sektorach pamięci karty.

Tryb autonomiczny

W *Trybie autonomicznym* zamek przyznaje dostęp do pomieszczenia w oparciu o karty zbliżeniowe zapisane w jego pamięci. Zamek może być na stałe skonfigurowany do pracy w *Trybie autonomicznym* lub automatycznie przechodzić do niego z *Trybu sieciowego*, gdy wystąpi awaria połączenia radiowego z koncentratorem.

W zamku można zdefiniować 100 kart zbliżeniowych. Każda z tych kart może mieć uprawnienie do chwilowego otwarcia drzwi (*Dostęp chwilowy*) oraz uprawnienie do trwałego otwarcia drzwi (*Dostęp biurowy)*. Gdy karta ma uprawnienie *Dostęp chwilowy* to jej użycie powoduje chwilowe odblokowanie przejścia na czas określony przez parametr *Czas odblokowania*. Gdy karta posiada uprawnienie *Dostęp biurowy*, użycie karty na przemian załącza i wyłącza *Tryb biurowy*. Gdy *Tryb biurowy* jest załączony, zamek jest na stałe odblokowany (klamka zewnętrzna jest zasprzęglona) i otwarcie drzwi nie wymaga użycia karty. Gdy *Tryb biurowy* jest wyłączony, przyznanie dostępu wymaga użycia karty. Możliwe jest nadanie karcie obydwu uprawnień (*Dostęp chwilowy* oraz *Dostęp biurowy*). W takim przypadku, w momencie pierwszego odczytu karty zamek przyznaje dostęp chwilowy natomiast, drugie użycie karty następujące bezpośrednio po pierwszym, załącza *Tryb biurowy*.

Dostęp do pomieszczenia od zewnątrz może być blokowany przy pomocy pokrętła umieszczonego na szyldzie wewnętrznym. Działanie tego pokrętła może być zablokowane przy pomocy nastawy *Nie przeszkadzaj*.

Karty rezerwowe

W zamku można zapamiętać 100 kart zbliżeniowych. Każda z tych kart może należeć do innego użytkownika. Opcjonalnie, zamek może pracować z liczbą użytkowników ograniczoną o połowę, tzn. do 50. W takim przypadku każdy użytkownik może posiadać dwie karty: *Kartę główną* i *Kartę rezerwową*. Obydwie karty mają te same uprawnienia, przy czym programowanie *Karty rezerwowej* może być pominięte. Fabrycznie nowy zamek jest skonfigurowany do trybu z 50 użytkownikami. Tryb ten jest też automatycznie ustawiany w procesie przywracania ustawień fabrycznych. Przełączenie zamka do trybu 100 użytkowników może nastąpić jedynie z poziomu programu RogerVDM. Główną zaletą stosowania *Kart rezerwowych* jest możliwość selektywnego wykasowania kart użytkownika z pamięci zamka pomimo braku ich dostępności (np. są zagubione lub zniszczone). Aby możliwe było późniejsze usunięcie wybranego użytkownika należy *Karty rezerwowe* opisać i złożyć w wybranym miejscu.

Uwaga: *Karta rezerwowa* posiada te same uprawnienia, co *Karta główna*.

Tryb sieciowy

W *Trybie sieciowym*, zamek jest połączony radiowo z kontrolerem dostępu, który steruje dostępem do pomieszczenia. Zarówno karty odczytane na zamku jak i stany jego linii wejściowych są raportowane do kontrolera, który zgodnie z konfiguracją systemu steruje zwrotnie zamkiem.

Domyślnie zamek pracuje w *Trybie autonomicznym*, w celu przełączenia do *Trybu sieciowego* należy pięciokrotnie zbliżyć kartę programującą *Usuń*. Opisaną procedurę można również wykorzystać w celu usunięcia aktualnie zapisanej konfiguracji sieci *RACS AIR*.

W przypadku utraty połączenia radiowego zamek samoczynnie przechodzi to *Trybu awaryjnego* (opis w sekcji *Przyznawanie dostępu w trybie awaryjnym).* Po odzyskaniu komunikacji radiowej zamek samoczynnie powraca do *Trybu sieciowego*.

Uwaga: Z natury rzeczy, systemy radiowe są zagrożone niestabilnością wynikającą z niepewnej łączności radiowej. Łączność ta może być zakłócana zarówno przez smog elektromagnetyczny istniejący w otoczeniu urządzeń jak i okresowo pojawiające się zakłócenia. Łączność radiowa może być również zakłócana celowo. Mając na uwadze wymienione zjawiska, w systemie kontroli dostępu RACS AIR przewidziano tzw. tryb awaryjny, który umożliwia podtrzymanie działania systemu w czasie braku łączności radiowej. Użytkowanie systemu bez skonfigurowanego trybu awaryjnego stwarza zagrożenie wystąpienia zakłóceń w jego działaniu, które to z kolei, mogą prowadzić do dużych utrudnień w użytkowaniu pomieszczeń objętych elektroniczną kontrolą dostępu.

Kanały radiowe

Komunikacja radiowa odbywa się w paśmie IEEE 802.15.4/ 2.4GHz, które jest współdzielone m.in. z sieciami Wi-Fi, które ze względu na dużą intensywność transmisji danych mogą zakłócić komunikację pomiędzy urządzeniem końcowym (np. zamkiem) a koncentratorem. Przed procesem budowy sieci, sprawdzenie należy sprawdzić, na jakich kanałach pracują okoliczne sieci Wi-Fi i wybranie takiego kanału radiowego lub grupy kanałów, które nie są zakłócone. Określenie zajętości kanałów radiowych można wykonać za pomocą dostępnych powszechnie aplikacji mobilnych typu „analizator Wi-Fi".

Uwaga: Należy mieć na uwadze, że pozytywny wynik testów nie jest gwarancją poprawnej pracy systemu gdyż zajętość pasma radiowego oraz poziom zakłóceń może ulegać znacznym zmianom (np. poprzez działanie nowych urządzeń z sąsiedztwa lub urządzeń mobilnych). W przypadku, gdy nie jest akceptowalne przełączenie systemu w tryb awaryjny na czas wystąpienia zakłóceń radiowych, proszę skorzystać z rozwiązań przewodowych w ramach systemu RACS5.

Podział pasma Wi-Fi (zgodnie z IEEE 802.11)			
Numer kanału	Przedział częstotliwości [GHz]	Numer kanału	Przedział częstotliwości [GHz]
1	2,401 - 2,423 (2,412)	8	2,436 - 2,458 (2,447)

2	2,406 - 2,428 (2,417)	9	2,441 - 2,463 (2,452)
3	2,411 - 2,433 (2,422)	10	2,446 - 2,468 (2,457)
4	2,416 - 2,438 (2,427)	11	2,451 - 2,473 (2,462)
5	2,421 - 2,443 (2,432)	12	2,456 - 2,478 (2,467)
6	2,426 - 2,448 (2,437)	13	2,461 - 2,483 (2,472)
7	2,431 - 2,453 (2,442)	14	2,473 - 2,495 (2,484)

Kanały radiowe RACS AIR (zgodnie z IEEE 802.15.4)			
Kanał	Częstotliwość [GHz]	Kanał	Częstotliwość [GHz]
11	2,405	19	2,445
12	2,410	20	2,450
13	2,415	21	2,455
14	2,420	22	2,460
15	2,425	23	2,465
16	2,430	24	2,470
17	2,435	25	2,475
18	2,440	26	2,480

Przyznawanie dostępu w trybie awaryjnym

Tryb awaryjny pozwala na funkcjonowanie przejść zbudowanych na zamkach bezprzewodowych podczas chwilowych zakłóceń komunikacji radiowej lub awarii systemu kontroli dostępu. Dostęp jest realizowany na podstawie danych zapisanych w pamięci czytnika:

Dynamiczna lista użytkowników

Dynamiczna lista kart budowana jest na bieżąco, podczas pracy systemu. Każda karta, która uzyskała dostęp do przejścia zgodnie z logiką kontrolera dostępu, zostaje zapisana na liście dynamicznej. Od tej pory, w trybie awaryjnym, odczyt karty znajdującej się na liście dynamicznej powoduje przyznanie dostępu. Po upływie czasu określonego przez parametr „Okres ważności karty użytkownika dynamicznego" karta zostaje automatycznie usunięta z listy, co pozwala na automatyczne usunięcie np. zgubionej lub nieaktywnej karty.

Lista użytkowników trybu autonomicznego

W trybie awaryjnym zamek korzysta z listy użytkowników trybu autonomicznego i podejmuje decyzje o przyznaniu dostępu zgodnie z opisem w sekcji :"Tryb autonomiczny".

Istnienie karty na dowolnej z ww. list jest warunkiem wystarczającym do przyznania dostępu w trbyie awaryjnym.

Wskaźniki LED

Zamek RWL-1 wyposażony jest w 4 diody sygnalizacyjne, których funkcje opisano w tabeli poniżej.

Wskaźniki LED		
Nazwa	Kolor	Opis
LED RED	Czerwony	W *Trybie sieciowym* funkcja tej diody podlega programowaniu z poziomu programu zarządzającego systemem kontroli dostępu VISO. W *Trybie autonomicznym* dioda miga, gdy zamek oczekuje na

		ponowne użycie identyfikatora. Jeśli to użycie nastąpi to zamek przełączy się do *Trybu biurowego*, w którym drzwi są na stałe odblokowane i wejście może odbyć się bez użycia identyfikatora.
LED GREEN	Zielony	W *Trybie sieciowym* funkcja tej diody podlega programowaniu z poziomu programu zarządzającego systemem kontroli dostępu VISO. W *Trybie autonomicznym* dioda ta nie jest wykorzystywana.
LED BLUE	Niebieski	W *Trybie sieciowym* sposób sterowania tym wskaźnikiem jest realizowany z poziomu kontrolera dostępu i jest zgodny z zasadami sterowania stosowanymi w systemie RACS 5. Jeśli na skutek awarii połączenia radiowego zamek przeszedł do pracy autonomicznej to sygnalizacja LED jest realizowana wg zasad obowiązujących w *Trybie autonomicznym* z tą różnicą, że ciągłe świecenie jest zastąpione szybkim miganiem wskaźnika. Wskaźnik wolno pulsuje przy braku konfiguracji sieci radiowej. W *Trybie autonomicznym* wskaźnik: • zapala się na 2s w momencie przyznania dostępu i zasprzęglenia klamki • świeci gdy zamek jest w *Trybie biurowym* • zapala się 2-krotnie na czas 2s w momencie odmowy dostępu
LED SYSTEM	Pomarańczowy	• świeci na stałe w przypadku rozprogramowania zamka • wolno pulsuje, gdy rozpoznano niski stan baterii i konieczna jest ich wymiana • błyska co 2s trakcie tworzenia połączenia z siecią

Zasilanie

Zamek zasilany jest z 4 baterii AA. Przy założeniu 10 odczytów dziennie, komplet nowych baterii alkaicznych wystarcza na ok. 2 lata pracy urządzenia. Niski stan baterii jest raportowany do oprogramowania zarządzającego systemem kontroli dostępu i dodatkowo sygnalizowany lokalnie przez miganie pomarańczowej diody oraz ciągły sygnał akustyczny generowany bezpośrednio przed przejściem zamka do uśpienia.

PROGRAMOWANIE

Zamek może być zaprogramowany manualnie, bez pomocy komputera lub przy użyciu komputera z programem narzędziowym RogerVDM. Programowanie manualne, umożliwia uproszczoną konfigurację zamka i jest ograniczone jedynie do możliwości dodania i usuwania użytkowników z zamka. Dostęp do wszystkich nastaw konfiguracyjnych zamkach jest możliwy wyłącznie z poziomu komputera. Programowanie z programu RogerVDM wymaga użycia interfejsu RUD-1.

Fabrycznie nowy zamek jest skonfigurowany do *Trybu autonomicznego* i dostarczany w komplecie z dwoma kartami programującymi (kartą DODAJ i kartą USUŃ). Czas otwarcia jest fabrycznie ustawiony na 2s a wbudowany czytnik skonfigurowany jest do odczytu seryjnego numeru karty (CSN).

Karty fabryczne		
Etykieta	**Nazwa**	**Uprawnienie**
ADD	Karta programująca DODAJ	Umożliwia dodanie nowej karty do pamięci czytnika
DEL	Karta programująca USUŃ	Umożliwia usunięcie karty z pamięci

		czytnika

Odczytywanie danych z zamka

W pewnych okolicznościach może zachodzić potrzeba odczytania danych z zamka. Operację tą można wykonać przy użyciu programu RogerVDM. Bez względu na tryb, w jakim pracuje zamek nie jest jednak możliwe odczytanie kluczy szyfrujących karty zbliżeniowe ani kluczy szyfrujących komunikację. Domyślnie, odczyt kart zaprogramowanych dla *Trybu autonomicznego* jest dozwolony, ale może być zabroniony za pomocą opcji *Blokada odczytu kart*.

Manualne programowanie użytkowników trybu autonomicznego

W przypadku, gdy zamek ma pracować jedynie w *Trybie autonomicznym*, możliwe jest jego skonfigurowanie manualne bez użycia komputera. Programowanie manualne umożliwia jedynie dodawanie i usuwanie kart z pamięci czytnika. Fabrycznie nowy czytnik jest wstępnie skonfigurowany do pracy autonomicznej i jest dostarczany w komplecie z zestawem 2 kart programujących. Karty programujące DODAJ i USUŃ można stosować zarówno w *Trybie autonomicznym* z listą 50 użytkowników jak i listą 100 użytkowników. W przypadku pracy z listą 100 użytkowników (tryb ten możliwy jest do ustawienia wyłącznie z programu RogerVDM) w procedurach opisanych poniżej zamek pomija krok, w którym programowana jest *Karta rezerwowa*.

Uwaga: Możliwe jest zaprogramowanie własnych kart programujących DODAJ i USUŃ w trakcie procedury przywracania ustawień fabrycznych.

Dodawanie użytkowników

A. Odczytaj kartę programującą DODAJ.

B. Odczytaj kartę, którą chcesz dodać; będzie to *Karta główna* nowego użytkownika.

C. Odczytaj kartę, która ma być *Kartą rezerwową* użytkownika zaprogramowanego w poprzednim kroku.

Uwagi:

- Jeśli chcesz, aby dodana mogła sterować *Trybem biurowym* to dwukrotnie wykonaj krok A.
- Jeśli chcesz, aby dodana karta sterować *Trybem biurowym* oraz jednocześnie umożliwiać dostęp chwilowy to trzykrotnie wykonaj krok A.
- Jeśli nie chcesz programować *Karty rezerwowej,* w kroku C odczytaj ponownie kartę programującą DODAJ.
- Jeśli w kroku B lub C nastąpi odczyt karty użytkownika, która już jest zaprogramowania zamek wygeneruje sygnał błędu (sygnał akustyczny 2s) i wyjdzie z programowania.

Przykład: Programowanie użytkownika uprawnionego do *Dostępu chwilowego*

- Odczytaj 1-krotnie kartę programującą DODAJ.
- Odczytaj kartę, którą chcesz dodać.
- Odczytaj kartę, która ma być *Kartą rezerwową.*
- Odczekaj do sygnału akustycznego złożonego z 3 bipów, po tym sygnale można kontynuować programowanie kolejnych kart.

Przykład: Programowanie użytkownika uprawnionego do sterowania *Trybem biurowym*

- Odczytaj 2-krotnie kartę programującą DODAJ.
- Odczytaj kartę, którą chcesz dodać.
- Odczytaj kartę, która ma być *Kartą rezerwową.*
- Odczekaj do sygnału akustycznego złożonego z 3 bipów, po tym sygnale można kontynuować programowanie kolejnych kart.

Przykład: Programowanie użytkownika uprawnionego do *Dostępu chwilowego* oraz sterowania *Trybem biurowym*

- Odczytaj 3-krotnie kartę programującą DODAJ.
- Odczytaj kartę, którą chcesz dodać.
- Odczytaj kartę, która ma być *Kartą rezerwową*.
- Odczekaj do sygnału akustycznego złożonego z 3 bipów, po tym sygnale można kontynuować programowanie kolejnych kart.

Usuwanie użytkowników

A. Odczytaj kartę programującą USUŃ.

B. Odczytaj *Kartę główną* lub *Kartę rezerwową* użytkownika by usunąć obie karty tego użytkownika z pamięci zamka.

Uwaga: Aby usunąć wszystkie karty z czytnika przywróć ustawienia fabryczne.

Przykład: Usuwanie użytkownika

- Odczytaj kartę programującą USUŃ.
- Odczytaj *Kartę główną* lub *Kartę rezerwową* użytkownika, którego chcesz usunąć.
- Odczekaj do sygnału akustycznego złożonego z 3 bipów, po tym sygnale można kontynuować programowanie lub usuwanie kolejnych kart.

Programowanie z poziomu program RogerVDM

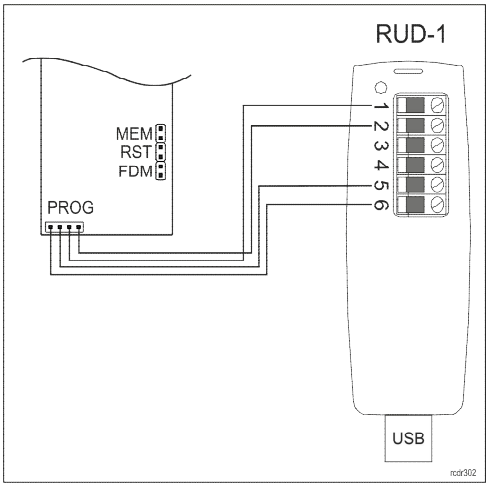
Program RogerVDM umożliwia skonfigurowanie zamka zarówno do pracy w *Trybie sieciowym* jak i *Trybie autonomicznym*. W przypadku użycia programu RogerVDM do obsługi czytnika, który ma pracować w *Trybie autonomicznym* możliwe jest umożliwia zarówno zaprogramowanie 100 użytkowników wyposażonych jedynie w *Kartę główną* jak i 50 wyposażonych w *Kartę główną* i *Kartę rezerwową*. Wybór pomiędzy trybem pracy z listą 100 lub 50 użytkowników dokonuje się przy pomocy nastawy *Karty rezerwowe*. Gdy opcja ta jest załączona czytnik pracuje z listą 50 użytkowników.

Uwaga: Zaleca się konfigurację zamka zapisać do pliku a dysku i zabezpieczyć przed utratą oraz dostępem osób postronnych.

Poniżej opisano sposób postępowania w celu wykonania programowania zamka z poziomu komputera.

1. Załóż zworkę na kontakty MEM.
2. Podłącz zamek do interfejsu RUD-1 przy użyciu dedykowanego kabelka (rys. 6).
3. Zewrzyj na chwilę kontakty RST – zacznie pulsować pomarańczowy wskaźnik LED.
4. W aplikacji RogerVDM wybierz *Urządzenie/Połącz* a następnie wybierz typ urządzenia (RWL-1) oraz wskaż port szeregowy, pod którym zainstalował się interfejs RUD-1.
5. Wybierz parametry konfiguracyjne zamka wg własnych potrzeb.
6. Zapisz ustawienia do pliku (komenda: *Zapisz do pliku*…).
7. Prześlij ustawienia do zamka (komenda: *Wyślij do urządzenia*…).
8. Wybierz polecenie *Urządzenie/Rozłącz*.
9. Usuń zworkę z kontaktów MEM.
10. Zewrzyj na chwilę kontakty RST.
11. Zamek jest gotowy do pracy.

Uwaga: Możliwe jest pozostawienie zworki na kontaktach MEM. W takim przypadku będzie możliwe w przyszłości przeprowadzenie bezprzewodowej konfiguracji zamka.



Rys. 7. Podłączenie zamka do interfejsu RUD-1

Polecenia programu RogerVDM

Poniżej wyjaśniono znaczenie podstawowych poleceń oferowanych przez program RogerVDM do obsługi zamka RWL-1.

Zakładka: Konfiguracja	
Wczytaj domyślne	Przywraca domyślne wartości parametrów w RogerVDM
Odczytaj z pliku..	Odczytuje zapisaną wcześniej konfigurację
Zapisz do pliku...	Zapisuje konfigurację do pliku
Odczytaj z urządzenia	Odczytuje konfigurację z urządzenia
Wyślij do urządzenia	Zapisuje konfigurację do urządzenia
Zakładka: Użytkownicy	
Dodaj	Dodaje nowego użytkownika
Edytuj	Edytuje istniejącego użytkownika
Usuń	Usuwa wybranego użytkownika
Usuń wszystko	Usuwa wszystkich użytkowników
Odczytaj z pliku..	Odczytuje listę użytkowników z pliku
Zapisz do pliku...	Zapisuje listę użytkowników z pliku
Odczytaj z urządzenia	Odczytuje listę użytkowników z urządzenia
Wyślij do urządzenia	Zapisuje listę użytkowników do urządzenia
Zakładka: Narzędzia	
Usuń konfigurację...	Usuwa konfigurację sieci RACS AIR

Parametry konfiguracyjne

Poniżej przedstawiono nastawy konfiguracyjnych zamka RWL-1. Wszystkie, wymienione poniżej parametry mogą być zmieniane z poziomu programu RogerVDM w trakcie niskopoziomowej konfiguracji urządzenia (zakładka: *Konfiguracja*).

Parametr	**Funkcja**
Ustawienia ogólne	

Tryb pracy	Parametr przełącza zamek pomiędzy *Trybem sieciowym* i *Trybem autonomicznym*. Wartość domyślna: *Tryb autonomiczny.*
Odczyt karty potwierdzony optycznie	Gdy opcja jest załączona, odczyt karty jest potwierdzany błyskiem na wskaźniku LED SYSTEM. Wartość domyślna: opcja wyłączona.
Odczyt karty potwierdzony akustycznie	Gdy opcja jest załączona, każdy odczyt karty jest potwierdzany krótkim bipem. Wartość domyślna: opcja wyłączona.
Zbliżenie karty potwierdzone optycznie	Gdy opcja jest załączona, LED SYSTEM pulsuje, gdy zamek rozpozna zbliżenie karty. Wartość domyślna: opcja wyłączona.
Sygnalizacja niskiego stanu baterii	Gdy opcja jest załączona, zamek sygnalizuje niski poziom baterii poprzez miganie LED SYSTEM oraz serią 5 bipów po odczycie karty. Wartość domyślna: opcja załączona.
Poziom głośności [%]	Parametr określa poziom głośności wbudowanego głośnika. Wartość zero wyłącza głośnik. Wartość domyślna: 100%
Tryb autonomiczny	
Czas otwarcia [s]	Parametr określa czas odblokowania zamka po rozpoznaniu karty. Wartość domyślna: 2s.
Karta programująca DODAJ	Karta zbliżeniowa służąca do dodawania nowych kart.
Karta programująca USUŃ	Karta zbliżeniowa służąca do usuwania kart.
Karty rezerwowe	Gdy opcja jest załączona zamek obsługuje 50 użytkowników a każdy z nich może mieć dwie karty (*Kartę główną* i *Kartę rezerwową*). Gdy opcja jest wyłączona zamek obsługuje 100 użytkownik z jedną kartą. Wartość domyślna: opcja załączona.
Blokada odczytu kart z urządzenia	Załączenie opcji blokuje możliwość odczytu kodów kart z czytnika za pośrednictwem programu RogerVDM. Wyłączenie blokady jest możliwe tylko przez przywrócenie ustawień fabrycznych. Opcja stosowana jest w celu uniemożliwienia odczytu kodów kart zapisanych w czytniku przez osoby postronne. Wartość domyślna: opcja wyłączona.
Nie przeszkadzaj	Załączenie opcji blokuje odczyt kart na wbudowanym czytniku zbliżeniowym po przekręceniu pokrętła na okuciu wewnętrznym. Każdorazowe otwarcie drzwi wyłącza blokadę (pokrętło wraca do stanu spoczynkowego). Wartość domyślna: opcja wyłączona.
Tryb sieciowy	
Ustawienia radiowe	
MAC urządzenia	Parametr wyświetla fabryczny numer identyfikacyjny zamka.
MAC koncentratora	Umożliwia wskazanie adresu MAC koncentratora, do którego zamek może się podłączyć.
Kanały radiowe	Lista kanałów radiowych, na których zamek może nawiązać łączność z koncentratorem. O ile nie jest to uzasadnione innymi względami, zaleca się nie ograniczać kanałów radiowych po stronie zamka, a wyboru kanału dokonać w koncentratorze sieci (RWH-1). Wartość domyślna: wszystkie kanały dostępne.
Identyfikator sieci	Parametr określa identyfikator sieci radiowej (tzw. PAN ID) w której będzie pracował zamek. Każda z sieci pracująca na tym samym kanale radiowym powinna mieć indywidualny PAN ID. Zakres dopuszczalnych wartości zawiera się w zakresie 0-16. Opcjonalnie, parametr może być ustawiany na wartość AUTO. W

	takim przypadku koncentrator samodzielnie wybiera numer PAN ID. Wartość domyślna: Auto.
Klucz szyfrujący	Klucz szyfrujący komunikację radiową. W przypadku wyboru wartości pustej, co jest preferowanym ustawieniem, klucz szyfrujący zostanie ustalony automatycznie w procesie budowy sieci. Wartość domyślna: Auto.
Czas notyfikacji [s]	Parametr określa czas, co jaki zamek samoczynnie wyjdzie z trybu uśpienia i połączy się z koncentratorem w celu potwierdzenia swojej obecności w sieci. Skracanie tego czasu przyśpiesza tempo wyczerpywania baterii zasilającej zamek. Wartość domyślna: 60s.
Czas rejestracji [s]	Parametr dotyczy procesu budowania sieci i określa czas, w ciągu którego należy odczytać dowolną kartę na zamku w celu ukończenia procesu dodania go do nowo-budowanej sieci. W przypadku przekroczenia tego czasu proces dodawania zamka należy rozpocząć na nowo. Wartość domyślna: 600s.
Czas ponownego wyszukania sieci [min.]	Czas po upływie, którego, zamek podejmie kolejną próbę połączenia się z koncentratorem, z którym utracił łączność. Wartość domyślna: 30min.
Kanał radiowy	Parametr wskazuje na kanał radiowy wykorzystywany przez sieć, w której pracuje znajduje się zamek.
Identyfikator sieci	Parametr wskazuje identyfikator sieci (PAN ID), w której znajduje się zamek.
Obsługa listy użytkowników dynamicznych	Załączenie opcji uruchamia działanie dynamicznej listy użytkowników, działającej zgodnie z opisem w sekcji „Przyznawanie dostępu w trybie awaryjnym”. Wartość domyślna: opcja załączona.
Okres ważności karty użytkownika dynamicznego	Określa czas, przez jaki będą ważne karty z listy dynamicznej (licząc od ostatniego przyznania dostępu przez kontroler). Wartość domyślna: 3600s.
Liczba przyznań dostępu przed dodaniem do dynamicznej listy użytkowników	Minimalna ilość przyznań dostępu przez kontroler, po których następuje zapis kodu karty na liście dynamicznej. W przypadku nastawy większej od jeden, kolejne odczyty zakończone przyznaniem dostępu muszą nastąpić w interwale określonym przez „Okres ważności karty użytkownika dynamicznego”. Wartość domyślna: 1.
Komentarze	
Komentarz do obiektu DEV	Dowolny tekst, którego celem jest opis obiektu. Komentarz ten pojawi się w programie zarządzającym systemem i ułatwi identyfikację obiektu. Obiekt DEV reprezentuje całe urządzenie (zamek jako całość). Wartość domyślna: RWL-1.
Komentarz do obiektu DEADBOLT	Dowolny tekst, którego celem jest opis obiektu. Komentarz ten pojawi się w programie zarządzającym systemem i ułatwi identyfikację obiektu. Obiekt DEADBOLT CONTACT reprezentuje wejście, do którego podłączone jest czujnik położenia rygla. Wartość domyślna: Deadbolt contact.
Komentarz do obiektu KNOB SWITCH	Dowolny tekst, którego celem jest opis obiektu. Komentarz ten pojawi się w programie zarządzającym systemem i ułatwi identyfikację obiektu. Obiekt KNOB SWITCH reprezentuje wejście, do którego podłączone jest pokrętło znajdujące się na wewnętrznym szyldzie zamka. Wartość domyślna: Knob switch.

Komentarz do obiektu DOOR CONTACT	Dowolny tekst, którego celem jest opis obiektu. Komentarz ten pojawi się w programie zarządzającym systemem i ułatwi identyfikację obiektu. Obiekt DOOR CONTACT reprezentuje wejście, do którego podłączone jest czujnik otwarcia drzwi. Wartość domyślna: Door contact.
Komentarz do obiektu LED RED	Dowolny tekst, którego celem jest opis obiektu. Komentarz ten pojawi się w programie zarządzającym systemem i ułatwi identyfikację obiektu. Obiekt LED RED reprezentuje wyjście sterujące stanem wskaźnika LED RED (czerwony). Wartość domyślna: LED red.
Komentarz do obiektu LED GREEN	Dowolny tekst, którego celem jest opis obiektu. Komentarz ten pojawi się w programie zarządzającym systemem i ułatwi identyfikację obiektu. Obiekt LED GREEN reprezentuje wyjście sterujące stanem wskaźnika LED GREEN (zielony). Wartość domyślna: LED green.
Komentarz do obiektu LED SYSTEM	Dowolny tekst, którego celem jest opis obiektu. Komentarz ten pojawi się w programie zarządzającym systemem i ułatwi identyfikację obiektu. Obiekt LED ORANGE reprezentuje wyjście sterujące stanem wskaźnika LED ORANGE (pomarańczowy). Wartość domyślna: LED system.
Komentarz do obiektu LOCK	Dowolny tekst, którego celem jest opis obiektu. Komentarz ten pojawi się w programie zarządzającym systemem i ułatwi identyfikację obiektu. Obiekt LOCK reprezentuje wyjście sterujące serwomechanizmem blokującym dostęp. Wartość domyślna: Lock.
Komentarz do obiektu BUZZER	Dowolny tekst, którego celem jest opis obiektu. Komentarz ten pojawi się w programie zarządzającym systemem i ułatwi identyfikację obiektu. Obiekt BUZZER reprezentuje wyjście sterujące wewnętrznym głośnikiem urządzenia. Wartość domyślna: Buzzer.
Komentarz do obiektu CDI	Dowolny tekst, którego celem jest opis obiektu. Komentarz ten pojawi się w programie zarządzającym systemem i ułatwi identyfikację obiektu. Obiekt CDI reprezentuje czytnik zbliżeniowy będący składnikiem urządzenia. Wartość domyślna: CDI.
Komentarz do obiektu PWR	Dowolny tekst, którego celem jest opis obiektu. Komentarz ten pojawi się w programie zarządzającym systemem i ułatwi identyfikację obiektu. Obiekt PWR reprezentuje źródło zasilania urządzenia, które w tym przypadku składa się z 4 baterii AA. Wartość domyślna: PWR.
Typy wejść	
Typ wejścia DEADBOLT	Parametr określa typ (NO lub NC) wejścia DEADBOLT. Wartość domyślna: NO.
Typ wejścia KNOB SWITCH	Parametr określa typ wejścia (NO/NC), do którego podłączone jest pokrętło na wewnętrznym szyldzie. Wartość domyślna: NO.
Typ wejścia DOOR CONTACT	Parametr określa typ (NO lub NC) wejścia DOOR CONTACT. Wartość domyślna: NC.
Czasy reakcji wejść	
Czas reakcji wejścia DEADBOLT	Parametr określa minimalny czas trwania impulsu na wejściu DEADBOLT, który zostanie zakwalifikowany, jako zmiana stanu wejścia. Wartość domyślna: 50ms.
Czas reakcji wejścia KNOB	Parametr określa minimalny czas trwania impulsu na wejściu KNOB

SWITCH [ms]	SWITCH, który zostanie zakwalifikowany, jako zmiana stanu wejścia. Wartość domyślna: 50ms.
Czas reakcji wejścia DOOR CONTACT	Parametr określa minimalny czas trwania impulsu na wejściu DOOR CONTACT, który zostanie zakwalifikowany, jako zmiana stanu wejścia. Wartość domyślna: 50ms.
Typ czytnika zbliżeniowego	
Typ czytnika	Parametr określa typ danych zwracanych przez czytnik kart zbliżeniowych do kontrolera. Na podstawie tego parametru kontroler dokonuje interpretacji kodu karty. Wartość domyślna: Numer 40bit.
Zaawansowane ustawienia odczytu kart	
CSNL	Parametr określa liczbę bajtów numeru seryjnego karty (CSN), które zostaną użyte do utworzenia wynikowego kodu karty (RCN). Wartość domyślna: 8.
Ustawienia MIFARE Classic	
Typ sektora	Gdy opcja jest załączona, wynikowy kod karty (RCN) zwracany przez czytnik będzie formowany z numeru programowalnego (PCN) zapisanego w pamięci karty oraz numeru seryjnego karty (CSN). Gdy opcja jest wyłączona, wynikowy kod karty (RCN) zwracany przez czytnik będzie formowany jedynie na bazie seryjnego kodu karty (CSN). Wartość domyślna: Brak.
Kodowanie	Format, w jakim zapisany jest numer PCN w bloku danych na karcie. Wartość domyślna: BIN.
Pozycja pierwszego bajtu (FBP)	Pozycja najstarszego bajtu (MSB) numeru PCN. Wartość domyślna: 0.
Pozycja ostatniego bajtu (LBP)	Pozycja najmłodszego bajtu (LSB) numeru PCN. Wartość domyślna: 7.
Numer sektora	Numer sektora danych na karcie gdzie przechowywany jest numer PCN. Wartość domyślna: 0.
Numer aplikacji (AID)	Numer aplikacji AID w sektorze MAD karty określający sektor, z którego odczytany jest kod PCN w przypadku wyboru sektora MSN. Wartość domyślna: 5156 (Roger AID).
Numer bloku	Numer bloku w sektorze, z którego odczytywany będzie numer PCN. Dla sektorów 0-31 dopuszczalne są bloki 0-2 a dla sektorów 32-39 bloki 0-14. Wartość domyślna: 0.
Typ klucza	Typ klucza szyfrującego dane na karcie. Wartość domyślna: Klucz typu A.
Klucz	6-bajtowy klucz szyfrujący dane na karcie. Wartość domyślna: FF...FF.
Ustawienia Mifare UltraLight	
Typ sektora	Gdy opcja jest załączona, wynikowy kod karty (RCN) zwracany przez czytnik będzie formowany z numeru programowalnego (PCN) zapisanego w pamięci karty oraz numeru seryjnego karty (CSN). Gdy opcja jest wyłączona, wynikowy kod karty (RCN) zwracany przez czytnik będzie formowany jedynie na bazie seryjnego kodu karty (CSN). Wartość domyślna: Brak.
Numer strony	Numer strony pamięci karty, z której odczytywany będzie numer

	PCN. Wartość domyślna: 0.
Ustawienia Mifare Plus	
Typ sektora	Gdy opcja jest załączona, wynikowy kod karty (RCN) zwracany przez czytnik będzie formowany z numeru programowalnego (PCN) zapisanego w pamięci karty oraz numeru seryjnego karty (CSN). Gdy opcja jest wyłączona, wynikowy kod karty (RCN) zwracany przez czytnik będzie formowany jedynie na bazie seryjnego kodu karty (CSN). Wartość domyślna: Brak.
Kodowanie	Format, w jakim zapisany jest numer PCN w bloku danych na karcie. Wartość domyślna: BIN.
Pozycja pierwszego bajtu (FBP)	Pozycja najstarszego bajtu (MSB) numeru PCN. Wartość domyślna: 0.
Pozycja ostatniego bajtu (LBP)	Pozycja najmłodszego bajtu (LSB) numeru PCN. Wartość domyślna: 7.
Numer sektora	Numer sektora danych na karcie gdzie przechowywany jest numer PCN. Wartość domyślna: 0.
Numer aplikacji (AID)	Numer aplikacji AID w sektorze MAD karty określający sektor, z którego odczytany jest kod PCN w przypadku wyboru sektora MSN. Wartość domyślna: 5156 (Roger AID).
Numer bloku	Numer bloku w sektorze, z którego odczytywany będzie numer PCN. Dla sektorów 0-31 dopuszczalne są bloki 0-2 a dla sektorów 32-39 bloki 0-14. Wartość domyślna: 0.
Typ klucza	Typ klucza szyfrującego dane na karcie. Wartość domyślna: Klucz typu A.
Klucz	16-bajtowy klucz szyfrujący dane na karcie. Wartość domyślna: FFF...FFF.
Ustawienia Mifare DesFire	
Typ sektora	Gdy opcja jest załączona, wynikowy kod karty (RCN) zwracany przez czytnik będzie formowany z numeru programowalnego (PCN) zapisanego w pamięci karty oraz numeru seryjnego karty (CSN). Gdy opcja jest wyłączona, wynikowy kod karty (RCN) zwracany przez czytnik będzie formowany jedynie na bazie seryjnego kodu karty (CSN). Wartość domyślna: Brak.
Kodowanie	Format, w jakim zapisany jest numer PCN w bloku danych na karcie. Wartość domyślna: BIN.
Pozycja pierwszego bajtu (FBP)	Pozycja najstarszego bajtu (MSB) numeru PCN. Wartość domyślna: 0.
Pozycja ostatniego bajtu (LBP)	Pozycja najmłodszego bajtu (LSB) numeru PCN. Wartość domyślna: 7.
Numer aplikacji (AID)	Numer aplikacji AID w sektorze MAD karty określający sektor, z którego odczytany jest kod PCN w przypadku wyboru sektora MSN. Wartość domyślna: 5156 (Roger AID).
Identyfikator pliku (FID)	Parametr określa identyfikator pliku w aplikacji AID: 0-16 dla MF DESFire EV0, 0-32 dla MF DESFire EV1. Wartość domyślna: 0.
Szyfrowanie komunikacji	Parametr określa sposób szyfrowania komunikacji pomiędzy kartą a czytnikiem. Wartość domyślna: Brak.

Numer klucza	Parametr określa numer klucza dostępu do danych na karcie. Wartość domyślna: 0.
Typ klucza	Parametr określa typ klucza szyfrującego dane na karcie. Wartość domyślna: TDES Native
Klucz	Klucz szyfrujący dane na karcie. Dla klucza typu 3KTDES, wymagane są 24 bajty, dla pozostałych kluczy (TDES i AES) wymagane jest 16 bajtów. Wartość domyślna: FF...FF.

Użytkownicy

Zakładka *Użytkownicy* pozwala na zarządzanie listą użytkowników, którzy posiadają uprawnienia dostępu w *Trybie autonomicznym*. W zależności od wartości parametru *Karty zapasowe* można w zamku zaprogramować 50 lub 100 użytkowników. Dodatkowo, dla każdego z użytkowników można ustawić opcję *Dostęp chwilowy* oraz *Dostęp biurowy*. Gdy użytkownik na załączoną opcję *Dostęp chwilowy* jest on uprawniony do dostępu chwilowego. Gdy użytkownik na załączoną opcję *Dostęp biurowy* jest on uprawniony do sterowania *Trybem biurowym*. Możliwe jest załączenie obydwu opcji. W takim przypadku po pierwszym użyciu karty zamek przyznaje dostęp chwilowy natomiast, gdy bezpośrednio po nim nastąpi drugie użycie karty, załącza zamek do *Trybu biurowego*. Jeśli zamek znajdował się już w *Trybie biurowym* to użycie karty z opcją *Dostęp biurowy* natychmiast po pierwszym użyciu przełącza zamek do *Trybu normalnego*.

Uwaga: Lista użytkowników zapisana w pamięci zamka jest również wykorzystywana w trakcie awarii połączenia radiowego, w czasie której zamek samoczynnie przechodzi z *Trybu sieciowego* do *Trybu autonomicznego*.

Przywracanie ustawień fabrycznych

Przywracanie ustawień fabrycznych umożliwia skasowanie pamięci wewnętrznej czytnika w tym kasowanie wszystkich zaprogramowanych kart i odtworzenia domyślnych nastaw urządzenia. Po resecie pamięci zamek ustawia się w *Trybie autonomicznym* z listą 50 użytkowników oraz pracę z 40 bitowym numerem seryjnym karty (CSN). W przypadku potrzeby przywrócenia ustawień fabrycznych zamka należy postępować wg procedury przedstawionej poniżej:

- Usuń zworkę z kontaktów MEM (o ile jest założona).
- Zewrzyj na chwilę kontakty RST.
- Podczas trwania sygnalizacji akustycznej, załóż zworkę na kontakty MEM, urządzenie potwierdzi przywrócenie ustawień fabrycznych 2-krotnym bipem.
- Odczytaj kartę zbliżeniową, która ma być nową kartą programującą DODAJ.
- Odczytaj kartę zbliżeniową, która ma być nową kartą programującą USUŃ.
- Odczekaj do sygnału akustycznego złożonego z 3 bipów. Po tym sygnale zamek kończy proces przywracania ustawień fabrycznych i przechodzi do normalnej pracy.

Uwaga: Jeśli zamek jest przewidziany do pracy w Trybie sieciowym, należy dodatkowo pięciokrotnie odczytać kartę programującą *Usuń*.

INSTALACJA

Okucie przeznaczone jest do montażu na drzwiach o grubości od 38 do 55mm oraz o rozstawie zamka wpuszczanego wynoszącym 72mm. Przed przystąpieniem do montażu należy sprawdzić czy posiadana wkładka patentowa ma odpowiednią długość.

Możliwy jest montaż na drzwiach przeciwpożarowych EI30 bez obniżenia ich klasyfikacji ogniowych po spełnieniu warunków:

- Drzwi drewniane pełne o grubości minimum 50mm (przylgowe lub bezprzylgowe).

- Otworowanie zgodnie z załączonym szablonem montażowym.
- Montaż drzwi zgodnie z zaleceniami producenta drzwi.

Montaż zamka

- Korzystając z dołączonego szablonu montażowego, należy wykonać otworowanie skrzydła drzwiowego. W przypadku montażu na drzwiach bezprzylgowych, może być konieczne użycie dołączonej blachy przylgowej.
- W drzwiach należy zamontować dostarczony zamek wpuszczany, zwracając uwagę aby znaki określające poprawne ustawienie łoża trzpienia klamki pokrywały się ze sobą (rys. 6). Wiązki K i L należy przeciągnąć przez górny otwór na stronę okucia zewnętrznego.
- Dzielony trzpień klamki (2 szt.) należy zamontować w zamku wpuszczanym (nacięciami w stronę zamka).
- Opcjonalnie należy zamontować czujnik otwarcia drzwi (np. kontraktron) i podłączyć do wiązki F (rys. 3).
- Przewody baterii oraz przełącznika strony wewnętrznej (rys. 5 poz. I i M) należy przeciągnąć przez dolny otwór, a następnie połączyć ze sobą poszczególne wiązki kablowe.
- Zamontować baterie (4xAA) w koszyku, a następnie wsunąć go w okucie wewnętrzne.
- Przykręcić okucie i sprawdzić działanie klamki po stronie wewnętrznej oraz wkładki patentowej, ze szczególnym uwzględnieniem cofania zatrzasku klamki za pomocą klucza.

Uwaga: Należy zabezpieczyć dostęp do klucza mechanicznego na wypadek konieczności awaryjnego otwarcia drzwi.

Dane techniczne

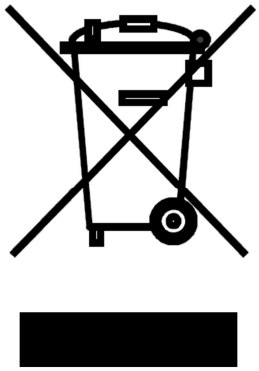
Parametr	Wartość
Zasilanie	4 baterie alkaiczne AA (LR06)
Trwałość kompletu baterii	2 lata przy 10 odczytach dziennie
Grubość drzwi	38 – 55 mm
Rozstaw zamka	72 mm
Komunikacja radiowa	Komunikacja bezprzewodowa zgodna z standardem IEEE 802.15.4/ 2.4GHz; zasięg transmisji do 10m
Wbudowany czytnik zbliżeniowy	Czytnik kart ISO/IEC 14443A MIFARE® Ultralight, Classic, DESFire EV1, Plus
Klasa środowiskowa (wg EN 50131-1)	Klasa I, warunki wewnętrzne, temp. +5°C - +40°C, wilgotność względna: 10..95% (bez kondensacji)
Stopień ochrony	IP40
Wymiary okucia	78 x 242mm
Rozstaw zamka wpuszczanego	72mm
Waga	Ok. 2200g
Certyfikaty	Znak CE, EI30 (patrz: montaż)

Oznaczenia handlowe

Produkt	Opis
RWH-1	Koncentrator systemu bezprzewodowego RACS 5 AIR
RWL-1-LI	Zamek bezprzewodowy z okuciem; drzwi prawe otwierane do wnętrza
RWL-1-RI	Zamek bezprzewodowy z okuciem; drzwi lewe otwierane do wnętrza
RWL-1-LO	Zamek bezprzewodowy z okuciem; drzwi lewe otwierane na zewnątrz
RWL-1-RO	Zamek bezprzewodowy z okuciem; drzwi prawe otwierane na zewnątrz

Historia produktu

Wersja produktu	Data wprowadzenia	Opis
1.0	IX 2017r.	Pierwsza wersja komercyjna produktu
1.1	VII 2019r	Dodana lista użytkowników dynamicznych

	Symbol ten umieszczony na produkcie lub opakowaniu oznacza, że tego produktu nie należy wyrzucać razem z innymi odpadami gdyż może to spowodować negatywne skutki dla środowiska i zdrowia ludzi. Użytkownik jest odpowiedzialny za dostarczenie zużytego sprzętu do wyznaczonego punktu gromadzenia zużytych urządzeń elektrycznych i elektronicznych. Szczegółowe informacje na temat recyklingu można uzyskać u odpowiednich władz lokalnych, w przedsiębiorstwie zajmującym się usuwaniem odpadów lub w miejscu zakupu produktu. Gromadzenie osobno i recykling tego typu odpadów przyczynia się do ochrony zasobów naturalnych i jest bezpieczny dla zdrowia i środowiska naturalnego. Masa sprzętu podana jest w instrukcji obsługi produktu.

Kontakt:
Roger sp. z o.o. sp.k.
82-400 Sztum
Gościszewo 59
Tel.: +48 55 272 0132
Faks: +48 55 272 0133
Pomoc tech.: +48 55 267 0126
Pomoc tech. (GSM): +48 664 294 087
E-mail: biuro@roger.pl
Web: www.roger.pl