

## Roger Access Control System 5

Nota aplikacyjna nr 024

Wersja dokumentu: Rev. C

# Obsługa kart MIFARE w systemie RACS 5

## *Wprowadzenie*

Najbardziej rozpowszechnionym sposobem identyfikacji użytkowników systemu kontroli dostępu są karty zbliżeniowe. W ramach systemu RACS 5 można używać wiele rodzajów kart jednocześnie. W systemach o niskim poziomie bezpieczeństwa powszechnie używane są karty EM 125kHz. W systemach z wymaganym wyższym poziomem bezpieczeństwa stosowane są karty, których numer jest przechowywany w szyfrowanych sektorach pamięci np. karty MIFARE. W ofercie systemu RACS 5 znajduje się szeroka grupa czytników MIFARE, w tym czytniki kart DESFire EV1 i Plus oferujące najwyższy poziom bezpieczeństwa. Za wyjątkiem terminala MCT68ME, który umożliwia wyłącznie odczyt numeru seryjnego karty (tzw. CSN), wszystkie pozostałe czytniki serii MCT umożliwiają odczyt kodu karty z szyfrowanych sektorów pamięci (tzw. PCN).

---

Uwaga: Należy mieć na uwadze, że samo użycie kart MIFARE nie gwarantuje wysokiego poziomu bezpieczeństwa. Poziom ten uzyskuje się przez takie skonfigurowanie systemu, w którym kod karty będzie pobierany z szyfrowanych sektorów pamięci karty.

---

## *Nośniki*

W systemie RACS 5 przez pojęcie Nośnika rozumie się dowolny typ przedmiotu lub metodę, która umożliwia identyfikację użytkownika. Typowymi Nośnikami są karty zbliżeniowe, kody PIN, hasła, mobilne klucze elektroniczne, linie papilarne i inne formy identyfikacji biometrycznej. Rozróżnia się różne Typy nośników. Na definicję Typu nośnika skład się Typ danych oraz Klasa. Typ danych określa sposób interpretacji danych przesyłanych przez Nośnik (np. numer 24 bit, numer 32 bit, ciąg alfanumeryczny itd.). Klasa nośnika określa technologię użytą do przesyłania danych (Karta MIFARE 1k, karta EM 125 kHz, kod PIN, hasło itd.). W procesie rozpoznania Nośnika odczytanego z czytnika kontroler dostępu sprawdza jego Wartość (kod), Typ danych oraz Klasę. Jeśli wszystkie trzy elementy pasują do Nośnika przechowywanego w pamięci kontrolera to jest on uznawany za poprawny. W standardowych rozwiązaniach wykorzystuje się predefiniowane Typy nośników zarówno na poziomie programu RogerVDM jak też VISO. Istnieje również możliwość definiowania własnych typów na poziomie programu VISO.

---

Uwaga: W definicji Typu nośnika w systemie RACS 5 (VISO) istnieje możliwość załączenia opcji *Bez klasy*, która powoduje, że kontroler pomija sprawdzanie Klasy nośnika i akceptuje Nośniki jedynie po sprawdzeniu ich Wartości oraz Typu danych.

---

## *Identyfikatory*

W systemie RACS 5 przez pojęcie Identyfikatora rozumie się grupę złożoną z jednego lub więcej Nośników. Odczyt dowolnego z Nośników jednoznacznie wskazuje Użytkownika, do którego on

należy. Wszystkie Nośniki w ramach tego samego Identyfikatora są równoprawne i mogą być używane zamiennie.

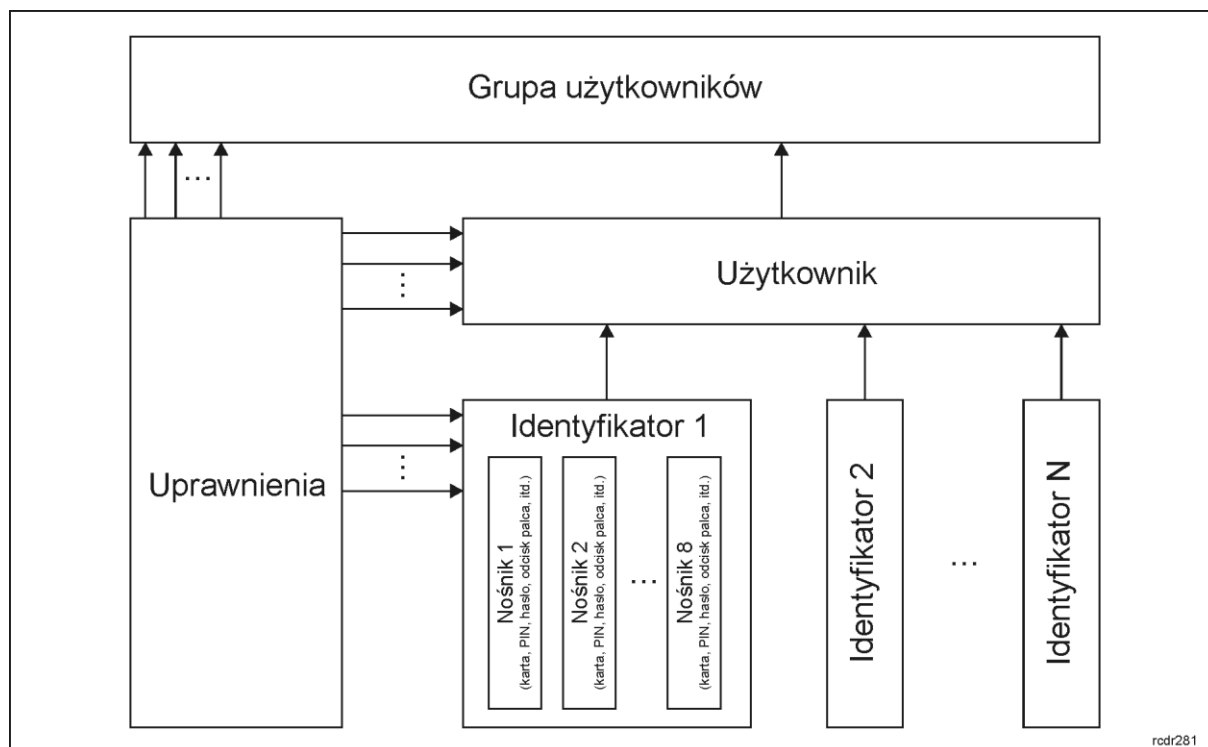
W systemie RACS 5 sposób rozpoznania Użytkownika określa tzw. Tryb logowania. W ramach Trybu logowania określone są Typy nośników, jakie Użytkownik musi użyć na Punkcie logowania (czytniku), kolejność ich użycia a także dopuszczalny czas na wprowadzenie Nośnika. Popularnymi Trybami logowania są tryby: Karta i PIN, Karta lub PIN, Karta i Odcisk palca. System udostępnia kilka typowych Trybów logowania oraz umożliwia tworzenia własnych, także takich które zawierają więcej niż dwa Typy Nośników (np. Karta i PIN lub Odcisk palca).

W systemie RACS 5 Uprawnienia (np. prawa dostępu) przypisywane są do Identyfikatorów, Grup użytkowników i/lub Użytkowników. Każdy Nośnik wchodzący w skład Identyfikatora dziedziczy wszystkie Uprawnienia przypisane do Identyfikatora. Użytkownik systemu może posiadać wiele Identyfikatorów a każdy z nich może składać się z wielu Nośników.

### ***Powiązania logiczne związane z Identyfikatorami***

Na rysunku poniżej przedstawiono w sposób schematyczny powiązania logiczne pomiędzy Grupą użytkowników, Użytkownikiem systemu, Identyfikatorami, Nośnikami oraz Uprawnieniami. Zachodzą następujące zależności:

- Użytkownik systemu może posiadać wiele Identyfikatorów.
- Każdy z Identyfikatorów może składać się z maks. 8 Nośników.
- Każdy Nośnik umożliwia jednoznaczną identyfikację Użytkownika.
- Uprawnienia mogą być przypisywane do Grupy użytkowników, Użytkownika oraz Identyfikatora
- Wynikowe uprawnienia Użytkownika są sumą jego własnych Uprawnień, tych, które dziedziczy z Grupy do której należy oraz Uprawnień przypisanych do Identyfikatora, który użył w celu identyfikacji.



Rys. 1 Powiązania logiczne pomiędzy Grupą, Użytkownikiem, Identyfikatorem, Nośnikami i Uprawnieniami

## Kod karty

W ogólnym przypadku kod karty MIFARE zwracany przez czytnik do kontrolera dostępu (tzw. RCN – Returned Card Number) może powstawać przez złożenie dwóch numerów odczytanych z karty: Sekcji CSN oraz Sekcji PCN ( $RCN = \text{Sekcja CSN} + \text{Sekcja PCN}$ ). Występowanie obydwu składników w wynikowym numerze karty nie jest obligatoryjne i numer RCN może zawierać tylko jedną z tych sekcji.

W przypadku, gdy system skonfigurowany jest do pracy z numerem RCN zawierającym sekcję PCN to karty pochodzące z innych systemów z innymi formatami RCN nie będą w ogóle odczytywane. Karty wykorzystujące sekcję PCN muszą być wcześniej zaprogramowane przez obsługę systemu. Programowanie numeru PCN można przeprowadzić przy wykorzystaniu dowolnego programatora kart. W ramach systemu RACS 5 oferowane są czytniki serii RUD (np. RUD-3, RUD-4), które udostępniają funkcję programowania kart. Programowanie numeru PCN kart może być wykonywane bezpośrednio z poziomu programu VISO służącego do konfiguracji i obsługi systemu lub programu narzędziowego RogerVDM. Domyślnie, terminale dostępu serii MCT przeznaczone do wykorzystania w systemie RACS 5 są skonfigurowane do odczytu kodu CSN ( $RCN = CSN$ ).

Uwaga: Numer PCN może być zaszyfrowany i przez to zabezpieczony przed modyfikacjami jak i nieuprawnionymi próbami odczytu. Zaleca się, aby systemy wymagające podwyższonego poziomu bezpieczeństwa bazowały na numerze PCN.

Aby czytnik prawidłowo odczytywał numer karty musi być skonfigurowany wg tych samych zasad, co czytnik programator użyty do ich programowania. Definicja numeru RCN wskazuje, w jaki sposób jest tworzony wynikowy kod karty.

RCN	
Sekcja CSN	Sekcja PCN

Uwaga: W prezentowanych poniżej przykładach mała litera „h” umieszczona na końcu ciągu cyfr oznacza zapis w systemie szesnastkowym.

## Sekcja CSN

Sekcja CSN to fragment numeru RCN, który pobierany jest z fabrycznie zaprogramowanego seryjnego numeru karty MIFARE (CSN). Sam numer CSN jest programowany w trakcie produkcji karty i nie może być później zmieniany. Numer CSN nie jest szyfrowany i może być powielany na innych kartach przy użyciu ogólnodostępnych programatorów.

Konfiguracja w zakresie sekcji CSN polega jedynie na wskazaniu ile bajtów numeru CSN ma być stosowane do formowania numeru RCN przez czytnik podczas odczytu karty. Definiuje się to za pomocą parametru *Długość numeru seryjnego karty (CSNL)* w programie RogerVDM w ramach konfiguracji niskopoziomowej danego czytnika serii RUD lub MCT. W zależności od typu karty numer CSN może zawierać 4 lub 7 bajtów danych. Parametr *CSNL* można ustawić w zakresie od 0 do 15 bajtów, co powoduje, że mogą zachodzić następujące przypadki szczególne:

- $CSNL = 0$  oznacza, że ani jeden bajt numeru CSN nie będzie użyty do uformowania numeru RCN i w efekcie numer ten w całości będzie uformowany z numeru PCN.
- Jeśli liczba dostępnych bajtów numeru CSN jest mniejsza od wartość parametru *CSNL* to brakujące pozycje są uzupełniane wiodącymi zerami.
- Jeśli wartość parametru *CSNL* jest mniejsza od liczby dostępnych bajtów w numerze CSN, to do uformowania numeru RCN będą użyte tylko najmłodsze (LSB) bajty numeru CSN.

### Przykład

Ustawiono  $CSNL = 5$  a numer CSN ma 4 bajty jak poniżej.

55h	66h	77h	88h
-----	-----	-----	-----

Sekcja CSN w numerze RCN będzie miała postać: 0055667788.

### Przykład

Ustawiono  $CSNL=2a$  numer CSN ma 4 bajty jak poniżej.

55h	66h	77h	88h
-----	-----	-----	-----

Sekcja CSN w numerze RCN będzie miała postać: 7788.

## Sekcja PCN

Sekcja PCN to fragment numeru RCN pobierany z programowalnych obszarów pamięci karty. Numer ten może być zaprogramowany przez użytkownika i zmieniany, jeśli zajdzie potrzeba. Numer PCN jest zapisany w indywidualnie wybranym sektorze karty oraz bloku, i może być zaszyfrowany przy pomocy klucza szyfrującego. Miejsce przechowywania numeru PCN na karcie definiuje nastawa *Typ sektora* w programie RogerVDM w ramach konfiguracji niskopoziomowej danego czytnika serii RUD lub MCT i może ona przybierać wartości *Brak*, *SSN*, *MAD* lub *Plik Desfire*.

Parametr Typ sektora	Sposób odczytu kodu PCN
Brak	Numer PCN nie jest brany pod uwagę. Wynikowy kod karty RCN jest formowany wyłącznie z numeru CSN.
SSN	Numer PCN jest odczytywany ze wskazanego sektora i bloku karty. Numer AID (Application ID) nie jest brany pod uwagę.
MSN	Numer PCN jest odczytywany ze wskazanego bloku w pierwszym napotkanym sektorze, który został oznaczony wskazanym w konfiguracji, dwubajtowym numerem AID. W przypadku, gdy więcej niż jeden sektor posiada podany numer AID, odczytany numer PCN będzie miał wartość przypadkową.
Plik Desfire	Numer PCN odczytywany jest z pliku wskazanego przez numer AID.

Liczba bajtów danych odczytywanych z pliku (dla kart Desfire) lub bloku danych (dla pozostałych kart) jest definiowana przez wskazanie pozycji pierwszego odczytywanego bajtu w bloku (parametr: *FBP*) oraz pozycji ostatniego bajtu w bloku (parametr: *LBP*). Przyjęło się, że jeżeli  $FBP > LBP$  to jest to kierunek normalny odczytu (Normal order) natomiast, jeśli  $FBP < LBP$  to jest to traktowane, jako kierunek odwrócony (Reverse order).

Numer PCN przechowywany na karcie może zostać zakodowany w postaci binarnej (*BIN*) lub tekstowej (*ASCII HEX*), a decyduje o tym parametr *Kodowanie*. W przypadku wyboru kodowania *ASCII HEX* jeden bajt danych przedstawia jeden znak w zapisie szesnastkowym np. '0100 0001' oznacza 'A' natomiast w formacie *BIN* te same bity oznaczają dwie cyfry szesnastkowe: 4 i 1 (41h). W przypadku kodowania *ASCII HEX* odczytana długość kodu PCN jest dwukrotnie mniejsza niż wynika z różnicy parametrów *FBP* oraz *LBP*. Parametry *FBP* i *LBP* są osobno definiowane dla kart Classic, Plus i Desfire. Parametry odczytu PCN z karty Ultralight są identyczne z nastawami kart Classic przy czym miejsce przechowywania numeru PCN dla tej karty jest stałe i nie ulega definiowaniu.

### Przykład

Ustawiono:  $FBP=5$ ,  $LBP=9$ ,  $Kodowanie=BIN$ . Blok danych zapisanych na karcie ma postać jak poniżej.

						<b>FBP</b>				<b>LBP</b>						
Poz.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
BIN	00h	11h	22h	33h	44h	55h	66h	77h	88h	99h	AAh	BBh	CCh	DDh	EEh	FFh

Odczytany numer PCN będzie miał postać: 5566778899.

### Przykład

Ustawiono  $FBP=9$ ,  $LBP=5$ ,  $Kodowanie=BIN$ . Blok danych zapisanych na karcie ma postać jak poniżej.

						<b>LBP</b>				<b>FBP</b>						
Poz.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
BIN	30h	31h	32h	33h	34h	35h	36h	37h	38h	39h	41h	42h	43h	44h	45h	46h

Odczytany numer PCN będzie miał postać: 3938373635.

### Przykład

Ustawiono  $FBP=3$ ,  $LBP=10$ ,  $Kodowanie=ASCII\ HEX$ . Blok danych zapisanych na karcie ma postać jak poniżej.

				<b>FBP</b>							<b>LBP</b>					
Poz.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ASCII	'0'	'1'	'2'	'3'	'4'	'5'	'6'	'7'	'8'	'9'	'A'	'B'	'C'	'D'	'E'	'F'
BIN	30h	31h	32h	33h	34h	35h	36h	37h	38h	39h	41h	42h	43h	44h	45h	46h

Odczytany numer PCN będzie miał postać: 3456789A.

### Przykład

Ustawiono  $FBP=2$ ,  $LBP=10$ ,  $Kodowanie=ASCII\ HEX$ . Blok danych zapisanych na karcie ma postać jak poniżej.

			<b>FBP</b>								<b>LBP</b>					
Poz.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ASCII	'0'	'1'	'2'	'3'	'4'	'5'	'6'	'7'	'8'	'9'	'A'	'B'	'C'	'D'	'E'	'F'
BIN	30h	31h	32h	33h	34h	35h	36h	37h	38h	39h	41h	42h	43h	44h	45h	46h

Odczytany numer PCN będzie miał postać: 23456789A.

### Przykład

Ustawiono  $FBP=10$ ,  $LBP=2$ ,  $Kodowanie=ASCII\ HEX$ . Blok danych zapisanych na karcie ma postać jak poniżej.

			<b>LBP</b>								<b>FBP</b>					
Poz.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ASCII	'0'	'1'	'2'	'3'	'4'	'5'	'6'	'7'	'8'	'9'	'A'	'B'	'C'	'D'	'E'	'F'
BIN	30h	31h	32h	33h	34h	35h	36h	37h	38h	39h	41h	42h	43h	44h	45h	46h

Odczytany numer PCN będzie miał postać: A98765432.

## Zasady tworzenia wynikowego kodu karty

Wynikowy kod karty (RCN) przesyłany z czytnika do kontrolera tworzony jest poprzez połączenie sekcji CSN oraz sekcji PCN i wyniku z następujących nastaw w programie RogerVDM: *Kodowanie*, *Typ sektora*, *AID*, *CSNL*, *FBP*, *LBP* oraz *Typ nośnika*.

### Przykład

Ustawiono  $CSNL=4$ ,  $FBP=8$ ,  $LBP=10$ ,  $Kodowanie=BIN$ . Sekcje CSN oraz PCN mają odpowiednio postacie jak poniżej.

Sekcja CSN=C4C5C6C7:

CSN						
C1h	C2h	C3h	C4h	C5h	C6h	C7h

Sekcja PCN=223344:

PCN																
Poz.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
BIN	AAh	BBh	CCh	DDh	EEh	FFh	00h	11h	22h	33h	44h	55h	66h	77h	88h	99h

Odczytany numer RCN będzie miał postać  $RCN=CSN+PCN=C4C5C6C7223344$ .

RCN						
Sekcja CSN				Sekcja PCN		
C4h	C5h	C6h	C7h	22h	33h	44h

Numer ten w zależności od nastaw parametru *Typ nośnika* może być transmitowany do kontrolera dostępu w zróżnicowany sposób. Poniżej podano kilka przykładów obrazujących różne warianty transmisji tego samego numeru  $RCN=C4C5C6C7223344h$  w zależności od rodzaju wybranego formatu wyjściowego czytnika.

### Przykład

Numer RCN wysłany przez czytnik z *Typem nośnika* ustawionym na *Numer 64 bit* będzie miał postać 00C4C5C6C7223344:

00h	C4h	C5h	C6h	C7h	22h	33h	44h
-----	-----	-----	-----	-----	-----	-----	-----

W przykładzie tym oryginalny numer RCN został uzupełniony dwoma wiodącymi zerami.

Numer RCN wysłany przez czytnik z *Typem nośnika* ustawionym na *Numer 40 bit* będzie miał postać C6C7223344:

C6h	C7h	22h	33h	44h
-----	-----	-----	-----	-----

W przykładzie tym oryginalny numer RCN został zredukowany o dwa wiodące bajty (C4h i C5h).

Numer RCN wysłany przez czytnik z *Typem nośnika* ustawionym na *Numer 24 bit* będzie miał postać 223344:

22h	33h	44h
-----	-----	-----

W przykładzie tym oryginalny numer RCN został zredukowany o cztery wiodące bajty (C4h, C5h, C6h i C7h).

Numer RCN odczytany przez czytnik serii PRT (system RACS 4) pracujący w trybie RACS CLK/DTA odczytuje 40 bitów kodu, co powoduje, że przykładowy numer RCN będzie miał postać C6C7223344:

C6h	C7h	22h	33h	44h
-----	-----	-----	-----	-----

W przykładzie tym oryginalny numer RCN został zredukowany o dwa wiodące bajty (C4h i C5h).

---

Uwaga:

1. Aby czytnik zwracał numer RCN składający się wyłącznie z numeru CSN należy w nastawach konfiguracyjnych czytnika ustawić parametr *Typ sektora=Brak* natomiast parametr *CSNL* ustawić na wartość różną od zera stosownie od ilości bajtów, które mają być brane pod uwagę przy analizie numeru karty przez kontroler.
  2. Aby czytnik zwracał wyłącznie numer karty zapisany w sektorze programowalnym PCN należy w nastawach konfiguracyjnych czytnika parametr *Typ sektora* ustawić na wartość inną niż *Brak* i jednocześnie parametr *CSNL* ustawić na zero.
  3. W przypadku, gdy skonfigurowany w czytniku numer RCN jest dłuższy niż długość kodu transmitowanego przez czytnik (parametr *Typ nośnika*) to czytnik pomija wiodące cyfry kodu RCN.
  4. W przypadku, gdy skonfigurowany w czytniku numer RCN jest krótszy niż długość kodu transmitowanego przez czytnik (parametr *Typ nośnika*) to czytnik uzupełnia kod RCN wiodącymi zerami.
- 

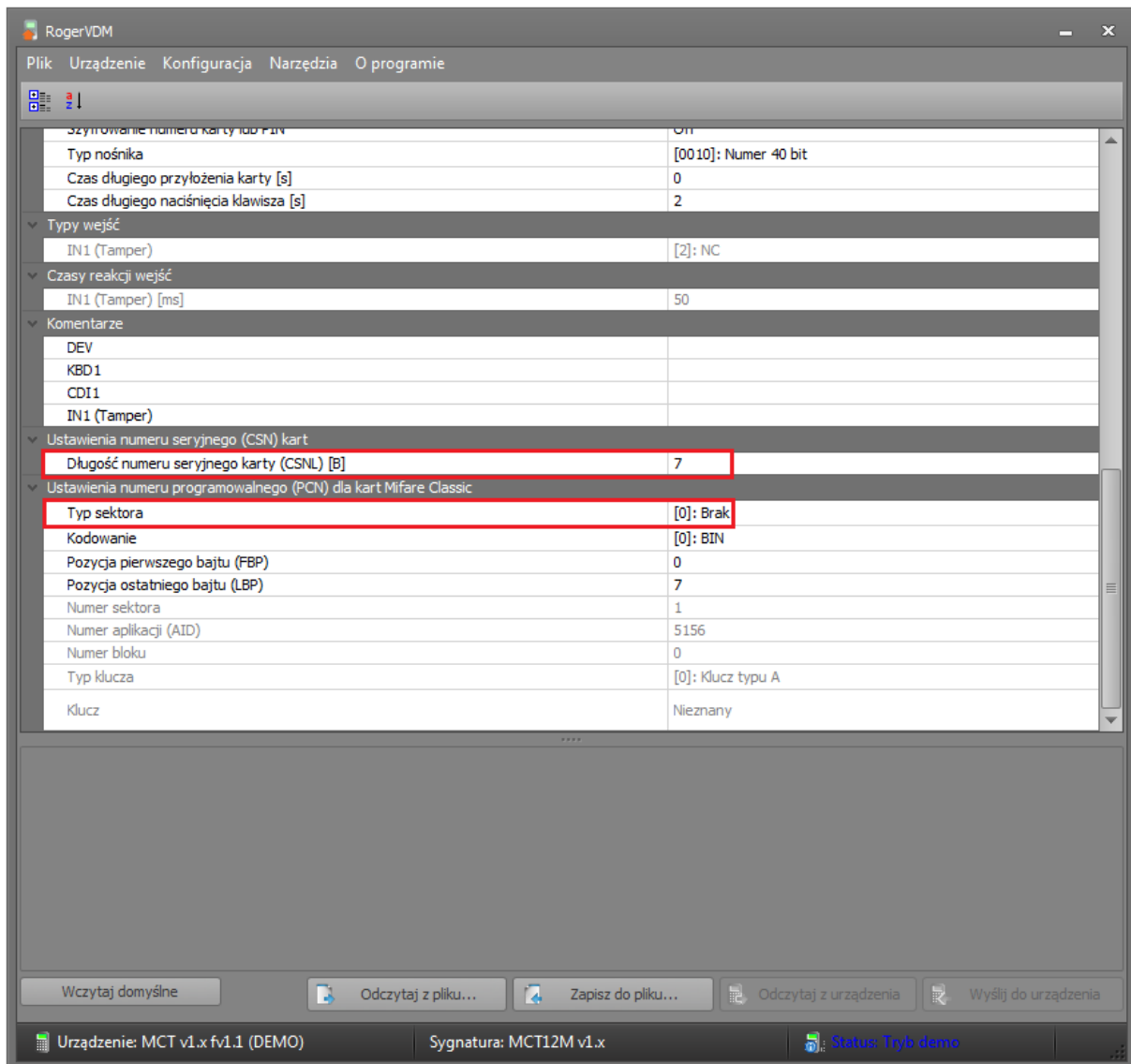
## Programowanie kart MIFARE

Domyślnie system RACS 5 bazuje na odczycie numerów seryjnych (CSN) kart MIFARE. W takim scenariuszu pracy nie jest konieczne definiowanie formatu numeru RCN jak też samych numerów PCN poszczególnych kart zbliżeniowych MIFARE. Programowanie numerów PCN kart podwyższa jednak poziom bezpieczeństwa bo znacznie utrudnia nieuprawnione kopiowanie kart użytkowników systemu RACS 5.

### Konfiguracja formatu numeru RCN

Konfiguracja formatu numeru RCN polega na określeniu parametrów Sekcji CSN oraz Sekcji PCN. Tą konfigurację wykonuje się w ramach konfiguracji niskopoziomowej czytnika systemu RACS 5. Wszystkie czytniki systemu (MCT i RUD) muszą mieć ustawiony taki sam format numeru RCN. Aby zdefiniować format RCN:

- Rozpocznij konfigurację niskopoziomową czytnika zgodnie z jego instrukcją instalacyjną.
- Po nawiązaniu połączenia z poziomu programu RogerVDM ustaw parametr *Długość numeru seryjnego karty (CSNL)* by zdecydować ile bajtów numerów CSN będzie użyte do tworzenia numeru RCN.
- W ramach ustawień numeru PCN danego typu karty MIFARE określ *Typ sektora* i w razie potrzeby pozostałe parametry w tym w szczególności *Typ klucz* oraz *Klucz* stosowany do szyfrowania numeru PCN.
- Ustaw te same parametry dla wszystkich pozostałych czytników MCT i RUD w systemie.



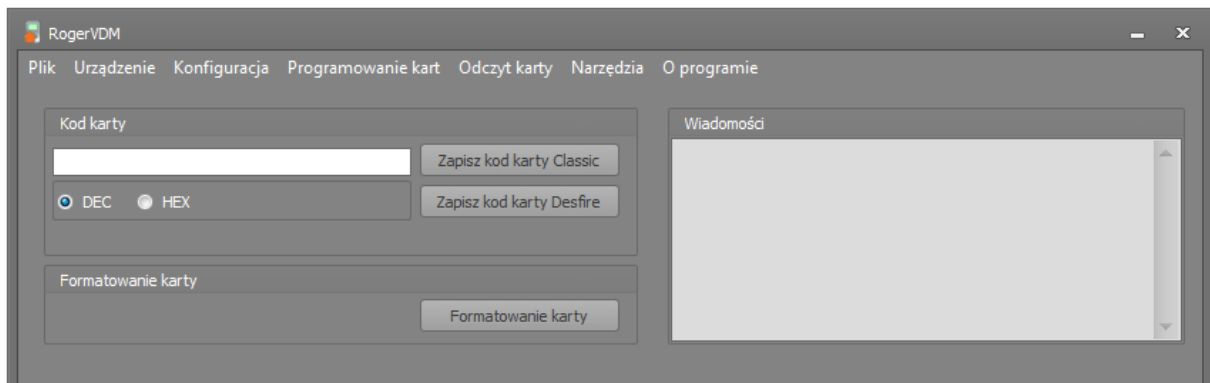
## Konfiguracja wartości numerów PCN

Numer PCN poszczególnych kart można definiować zarówno z poziomu programu narzędziowego RogerVDM jak też programu VISO do zarządzania systemem kontroli dostępu RACS 5.

### Konfiguracja numerów PCN z poziomu RogerVDM:

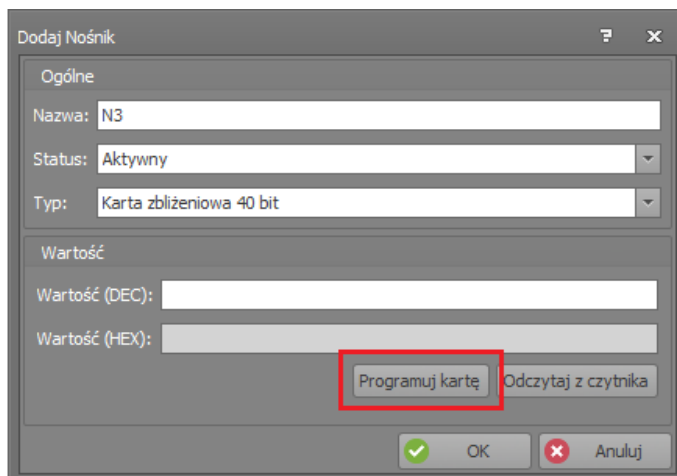
- Podłącz czytnik RUD-3 lub RUD-4 do portu USB komputera.
- Nawiąż połączenie z czytnikiem za pomocą programu RogerVDM tak jak w przypadku konfiguracji niskopoziomowej.
- Ustawienia formatu RCN czyli ustawienia numerów CSN i PCN czytnika RUD muszą być takie same jak pozostałych czytników w systemie. Te ustawienia zostaną wykorzystane podczas programowania kart.
- W menu górnym programu RogerVDM wybierz polecenie *Programowanie kart*.
- W otwartym oknie w razie potrzeby sformatuj kartę czyszcząc całkowicie jej pamięć (numer CSN nie jest usuwany z karty).
- Wprowadź własny numer w polu *Kod karty* i naciśnij przycisk zapisu w zależności od typu programowanej karty by zdefiniować numer PCN na karcie.
- Zaprogramuj kolejne karty w ten sam sposób, każdą z własnym numerem PCN.
- Zaprogramowane karty mogą być następnie użyte do definiowania Nośników użytkowników systemu za pomocą programu VISO.






#### Konfiguracja numerów PCN z poziomu VISO:


- Podłącz czytnik RUD-3 lub RUD-4 do portu USB komputera.
- Ustawienia formatu RCN czyli ustawienia numerów CSN i PCN czytnika RUD muszą być takie same jak pozostałych czytników w systemie. Te ustawienia zostaną wykorzystane podczas programowania kart.
- Uruchom program VISO i podczas definiowania Nośników jedną z dostępnych metod w oknie *Dodaj Nośnik* wybierz przycisk *Programuj kartę*.



- W nowo otwartym oknie wprowadź własny numer w jednym z pól obszar *Numer karty* lub wygeneruj numer losowy dostępnym przyciskiem. Następnie wybierz przycisk programowania karty w zależności od jej typu by rozpocząć zapis numeru PCN na karcie. Zamknij okno.
- Wybierz przycisk *Odczytaj z czytnika* by utworzyć Nośnik z właśnie zaprogramowaną kartą.
- Zaprogramuj kolejne karty w ten sam sposób, każdą z własnym numerem PCN.

Programowanie numeru karty

 Wybierz czytnik który będzie użyty do programowania.

 Odśwież listę urządzeń

Port	Numer seryjny	Opis	Urządzenie	Wersja firmware
▶ USB-HID	53330000F0F1C06	Mifare Card Reader	RUD-3-DES v2.0	2.0.4.023

Numer karty

DEC:

HEX:



ASCII:

Generuj numer losowy

Programuj kartę Mifare Classic

Programuj kartę Mifare Desfire

Numer ostatnio zaprogramowanej karty:

 OK  Anuluj

**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: [pomoc.techniczna@roger.pl](mailto:pomoc.techniczna@roger.pl)**  
**Web: [www.roger.pl](http://www.roger.pl)**