Roger Access Control System 5v2

Application note no. 024

Document version: Rev. B

MIFARE cards

Note: This document refers to RACS 5 v2.0.8 or higher

Introduction

The most common method of user identification in access control system is based on proximity cards/tokens. Multiple types of proximity cards can be used in RACS 5 concurrently. In low security systems, EM125kHz (UNIQUE) proximity cards are usually used. In high security systems, proximity cards which can store number in the encrypted sectors of their memory e.g. MIFARE® cards are usually used. Wide range of MIFARE readers is available in RACS 5 product portfolio, including high security MIFARE DESFire EV1/EV2/EV3 and MIFARE Plus readers. MCT68ME reader offers only card serial number (CSN) reading while all remaining MCT series readers enable also the reading of card number from encrypted sectors of card memory (PCN).

Note: It must be noted that the sole use of MIFARE proximity cards does not guarantee higher security as it is achieved when the system is configured to read card number from encrypted sectors (PCN) instead of using only card serial number (CSN).

Authentication Factors

In RACS 5 system, the Authentication Factor is an object or method used for user identification. Typical Authentication Factors are proximity cards, PINs, passwords, mobile keys, fingerprints and other forms of biometric identification. There are various Authentication Factor Types which are characterized by Type and Class. The Type defines method of data interpretation (e.g. 24 bit number, 32 bit number, alphanumeric string, etc.) while the Class defines technology of data transmission (e.g. MIFARE 1k card, EM125kHz card, PIN, password, etc.). In the identification process of card used at the reader, the access controller verifies the Value (number), Type and Class of Authentication Factor. If all three parameters are matched with the ones stored in the memory of access controller then the factor is deemed valid. In typical scenarios predefined Authentication Factor Types are applied both in RogerVDM and VISO programs but it is possible to define own types on the level of VISO software as well.

Note: When Authentication Factor Type is defined in RACS 5 system (VISO) then the option *No class* can be selected. In such case the access controller does not verify Class and the identification is then based only on Factor Value and Type.

Access Credentials

In RACS 5 system, the Access Credential is a group of one or more Authentication Factors. Each factor directly indicates a user it belongs to. All Authentication Factors within the same Access Credential have the same Authorisations and can be used interchangeably.

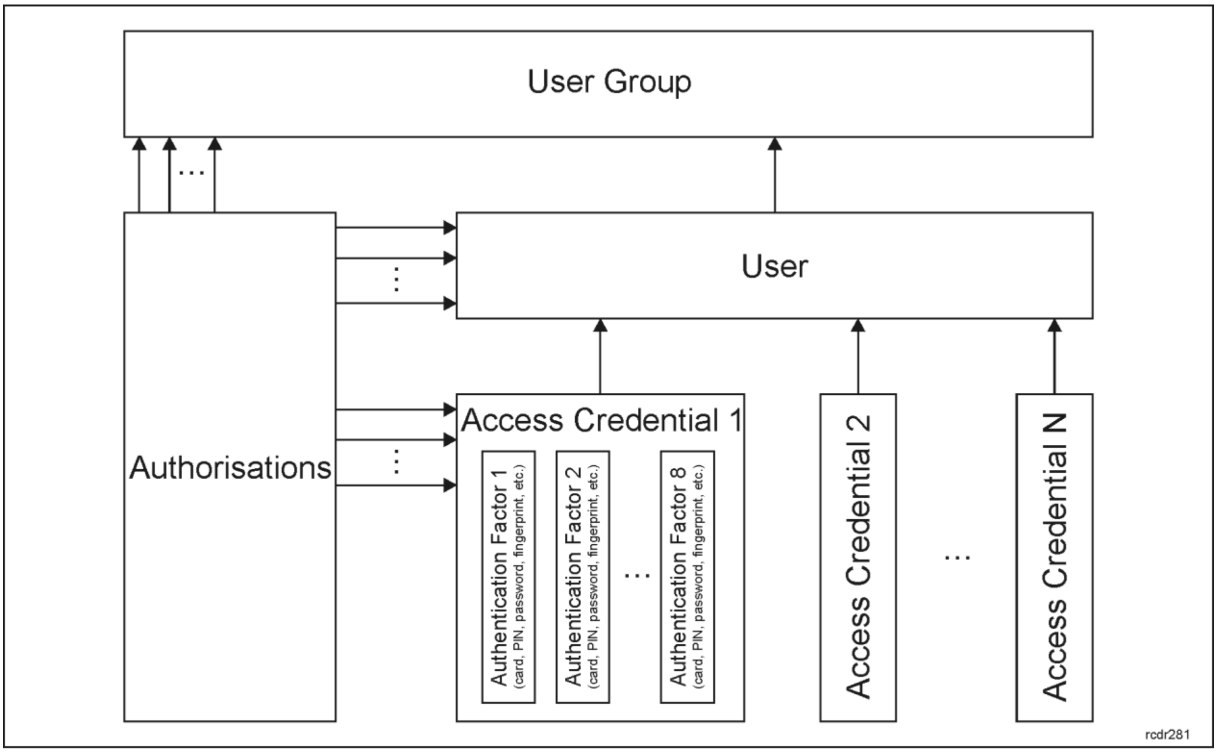
In RACS 5 system, the method of user recognizing is specified by Authentication Policy. Such policy defines Authentication Factor Types for identification of User at Access Point (reader) as well as their order of use and acceptable time for their use. The most commonly applied Authentication Policies are: Card and PIN, Card or PIN, Card and Fingerprint. The system offers some predefined policies but it is also possible to define own ones with more than two Authentication Factor Types (e.g Card and PIN or Fingerprint).

In RACS 5 system, the Authorisations (e.g. access rights) are assigned to Access Credentials, User groups and/or Users. Each Authentication Factor within certain Access Credential inherits all Authorisations assigned to the Access Credential. User can have multiple Access Credentials and each can consists of multiple Authentication Factors.

Logical connections related to Access Credentials

In the figure below logical connection of Access Credentials, Authentication Factors, User Group, User and Authorisations are shown. Following relations are effective:

- User can have multiple Access Credentials.
- Each Access Credential can include up to 8 Authentication Factors.
- Each Authentication Factor enables straight identification of User.
- Authorisations can be assigned on the level of User Group, User and Access Credential.
- Resultative rights of the User are the sum of Authorisations assigned to such User, Authorisations assigned to Group of the User and Authorisations assigned to Access Credential used for identification.


User Group
...
User
Authorisations
Access Credential 1
Authentication Factor 1 (card, PIN, password, fingerprint, etc.)
Authentication Factor 2 (card, PIN, password, fingerprint, etc.)
...
Authentication Factor 8 (card, PIN, password, fingerprint, etc.)
Access Credential 2
...
Access Credential N
rcdr281

Card number

RCN (Returned Card Number) which is transmitted by reader to access controller for the purpose of user identification consists of two sections corresponding to two numbers stored on MIFARE card i.e. read only CSN (Chip Serial Number) and custom PCN (Programmed Card Number). It is not obligatory to use both numbers for the composition of RCN as it may include only CSN section or only PCN section.

When the system is configured for the operation with RCN number which includes PCN section then cards from other systems with other definitions of RCN format will not be recognized at all by RACS 5 readers. Cards with PCN must be earlier programmed by administrator of the system. It can be done with card programmer e.g. RUD-3-DES using VISO software or RogerVDM software. By default MCT readers of RACS 5 system are configured for the reading of RCN with only CSN section (RCN=CSN).

Note: Encrypted PCN is protected against modifications and unauthorized reading. It is recommended to apply PCN in systems that require high security.

Any MCT reader must be configured with the same parameters as card writer used to program cards. The definition of RCN explains how the resulting card number is created from CSN and PCN sections of the card.

RCN	
CSN section	PCN section

Note: In the examples below the letter 'h' signifies hexadecimal number.

CSN section

CSN section can be a part of RCN and it is based on factory defined chip serial number of MIFARE card. CSN is read-only number. It is not encrypted and it can be copied on more cards with widely available programming devices.

In order to configure CSN section it is necessary to specify how many bytes of CSN will be used in RCN by reader when card is read. This is configured by means of the parameter *Serial number length (CSNL)* in RogerVDM or VISO v2 software during low level configuration of MCT, RUD or RFT1000 reader. Depending on MIFARE card type the CSN can include 4 or 7 bytes of data while the *CSNL* parameter can be configured in range of 0 to 15 bytes. Therefore following scenarios are possible:

- *CSNL=0* means that no CSN byte will be used in RCN so the RCN can be based solely on PCN section.
- If the number of CSN bytes in card memory is lower than *CSNL* parameter then leading zeros are used for missing bytes.
- If the *CSNL* parameter is lower than the number of CSN bytes then the CSN section of RCN will include only the least significant bytes (LSB) of CSN.

Example

If *CSNL=5* and CSN includes four bytes of data as below then CSN section of RCN is 0055667788.

55h	66h	77h	88h

Example

If *CSNL=2* and CSN includes four bytes of data as below then CSN section of RCN is 7788.

55h	66h	77h	88h

PCN section

PCN section can be a part of RCN and it is stored on card's memory. It is necessary to define PCN settings for card readers including the location of the section in memory and its security key before individual PCNs values are programmed on cards by administrator. Such configuration is done within low level configuration of a reader by means of RogerVDM or VISO v2 software. PCS section settings are applied both for card reading and card writing.

Sector type parameter decides if PCN is recognized and used by a reader.

Sector type	**PCN reading method**
NONE	PCN is omitted. RCN can be based solely on CSN.
SSN	PCN is used and it is possible to indicate where it will be stored in card memory (parameters *Sector ID* and *Block ID*) and to define how the access to PCN will be secured (parameters *Key type* and *Key*). SSN Sector type does not concern MIFARE DESFire cards.
MSN	PCN is used but its location is not indicated directly in card memory. Parameter *Application ID (AID)* which was officially registered by Roger company is used for this purpose. The same as in case of SSN, it is possible to define how the access to PCN will be secured (parameters *Key type* and *Key*). MSN Sector type does not concern MIFARE DESFire cards.
Desfire file	PCN is used and it is possible to indicate where it will be stored in card memory by defining own *Application ID (AID)* and *File ID (FID)*. It is also possible to define how the access to PCN will be secured (parameters *Key type* and *Key*). The parameter *Key number* is used only if it is necessary to adapt RACS 5 readers to MIFARE cards which are already programmed and used in other system. Desfire file sector type concerns only MIFARE DESFire cards.

Except for PCN location and its access key it is additionally necessary to define the number of data bytes read from file (for MIFARE Desfire cards) or data block (for remaining MIFARE cards) indicating first byte position in block (*FBP* parameter) and last byte position in block (*LBP* parameter). If *FBP<LBP* then the reading order is normal and if *FBP>LBP* then the reading order is reversed.

All PCN section settings including *FBP* and *LBP* parameters are defined separately for MIFARE Classic, Plus and DESFire formats. In case of MIFARE Ultralight only CSN is supported and when reader is configured for MIFARE Ultralight then only *CSNL* parameter should be configured while *Sector type* parameters for MIFARE Classic, Plus and DESFire should be set to *None*.

PCN can be stored on card in binary format (*BIN*) or text format (*ASCII HEX*) which is configured with *Format* parameter. If *ASCII HEX* format is selected then single byte represents character in hexadecimal format e.g. '0100 0001' corresponds to 'A' while in *BIN* format the same bytes can be presented as '41' hexadecimal number. In case of *ASCII HEX* format the length of PCN is two times shorter than it would result from difference of *FBP* and *LBP* parameters. Additionally when the number of ASCII HEX digits is uneven then leading zero is automatically added to the card number.

Example

If *FBP=5*, *LBP=9*, *Format=BIN* and data block is as below then PCN is 5566778899.

						FBP				**LBP**						
Pos.	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

Example

If *FBP=9*, *LBP=5*, *Format=BIN* and data block is as below then PCN is 3938373635.

						LBP				**FBP**						
Pos.	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

Example

If *FBP=3*, *LBP=10*, *Format=ASCII HEX* and data block is as below then PCN is 3456789A.

				FBP							**LBP**					
Pos.	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

Example

If *FBP=10*, *LBP=2*, *Format=ASCII HEX* and data block is as below then PCN is 0A98765432 where leading zero is added due to uneven number of digits in data block.

			LBP								**FBP**					
Pos.	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

RCN format rules

RCN (Returned Card Number) which is transmitted by reader to access controller consists of CSN section and PCN section while its value is specified by such parameters in RogerVDM software as: *CSNL, Sector type, Format*, *FBP* and *LBP*. At the same time the maximal length of RCN sent by MCT reader is 8 bytes (16 HEX digits) and sent by PRT readers is 5 bytes (10 HEX digits). Therefore the total number of RCN bytes configured for reader should not exceed these limits.

Note: In case of MCT readers with firmware v1.1.9.151 and newer, the length of RCN sent from reader to controller is not affected by *AF type* parameter and it results directly from RCN parameters.

Example

CSNL=4, *FBP=8*, *LBP=10*, *Format=BIN* while CSN and PCN sections are as below.

CSN on MIFARE card=C4C5C6C7

CSN						
C1h	C2h	C3h	C4h	C5h	C6h	C7h

PCN on MIFARE card=223344

PCN																
Pos.	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

RCN sent by MCT reader is RCN=CSN+PCN=C4C5C6C7223344 and it will not be reduced because it does not exceed 8 bytes.

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

RCN sent by PRT reader to access controller will be reduced to RCN=C6C7223344 because it exceeds 5 bytes.

RCN						
CSN section				PCN section		
		C6h	C7h	22h	33h	44h

Note:
1. The RCN returned by reader includes only CSN section if the parameter *Sector type=None* and the parameter *Serial number length (CSNL)* is in range of 1-7 depending on the number of bytes intended for identification.
2. The RCN returned by reader includes only PCN section if the parameter *Sector Type≠None* and the parameter *Serial number length (CSNL)=0*.

MIFARE card programming

In RACS 5 system, default identification is based on card serial number (CSN) reading. In such scenario it is not necessary to define RCN format and PCN values for all MIFARE proximity cards. However, cards programming with PCN significantly improves the security in the system and substantially prevents duplication of cards already configured in the system. According to description in previous sections, RCN can consist of CSN section and PCN section but in configuration examples below it is assumed that RCN = PCN so the CSN is not applied at all.

RCN format configuration

RCN format defines length, location, encryption, etc of card number. In order to configure RCN format for card programmer and readers:

- Connect card programmer (e.g. RUD-3-DES, RUD-4-DES) to computer’s USB port. RCN format must configured in the same way for all card programmers and readers in the system.
- Start low level configuration of the card programmer according to its Installation Manual.
- Configure the parameter *Serial number length (CSNL) = 0* so card serial number (CSN) will not be used at all.
- When configuring PCN format for particular type of MIFARE proximity card specify *Sector type* parameter and if needed also other parameters, in particular *Key type* and *Key* which define password for card number reading. Typical settings for MIFARE DESFire cards are given below.

Parameter	**Range**	**Value**
Serial number length (CSNL) [B]	0 - 8	0
Sector type	-	[1]: Desfire file
Format	-	[0]: BIN
First byte position (FBP)	-	0
Last byte position (LBP)	-	7
Application ID (AID)	6 HEX characters (0 – 9, A – F)	F51560
File ID (FID)	0 -31	0
Communication protection level	-	[2]: Full encryption

Key number	0 - 13	0
Key type	-	[3]: AES128
Key	32 HEX characters (0 – 9, A – F)	Own 32 characters password

- Configure the same settings for all other readers (MCT, OSR, PRT and RFT1000) in the system.

Note: In case of MIFARE Plus and MIFARE Classic cards the settings related to card number format are similar with the exception of *Sector type* parameter which should be set to *[1]: SSN*.

Note: In case of MCT readers with firmware v1.1.9.151 and newer, the parameter *AF Type* is irrelevant and the length of RCN sent from reader to controller results directly from RCN parameters. In case of OSR readers and MCI-3 interfaces the parameter *AF Type* should be configured with the same value (by default *[0010]: Number 40bits*) and Authentication Factors in VISO software should be defined accordingly.

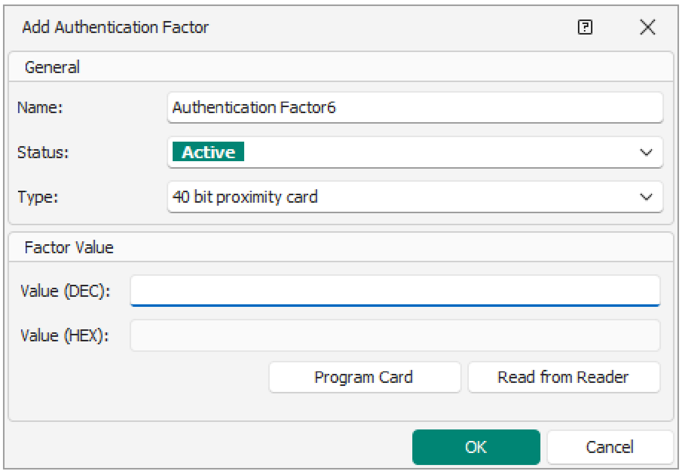
Note: When PCNs are applied then security in the system is higher and then it is also recommended to enable encryption for other transmissions to MC16 controller i.e. RS458 bus and OSDP bus. In such scenario for all devices on RS485 bus such as MC16 controller, MCT readers and MCI interfaces (if installed) there should be enabled the option *RS485 encryption* and there should be defined the parameter *RS485 encryption key*. Similarly in case of OSDP, for OSR readers and MCI-3 interfaces there should be enabled the option *OSDP encryption* and there should be defined the parameter OSDP password.

PCN programming

PCN is a programmable number which distinguishes particular card from other cards with their PCNs. Cards are assigned to Persons and then used for their identification in the access control system. It is recommended to program cards and then assign them to Persons using VISO software. Card programming can also be done with RogerVDM software.

PCN programming with VISO software:

- Connect card programmer (e.g. RUD-3-DES, RUD-4-Des) to computer's USB port. RCN format must configured in the same way for all card programmers and readers in the system.
- Start VISO program and when Authentication Factor is defined with one of available methods (e.g. Add Person Online wizard), select the button *Program Card*.



Add Authentication Factor

General

Name: Authentication Factor6

Status: Active

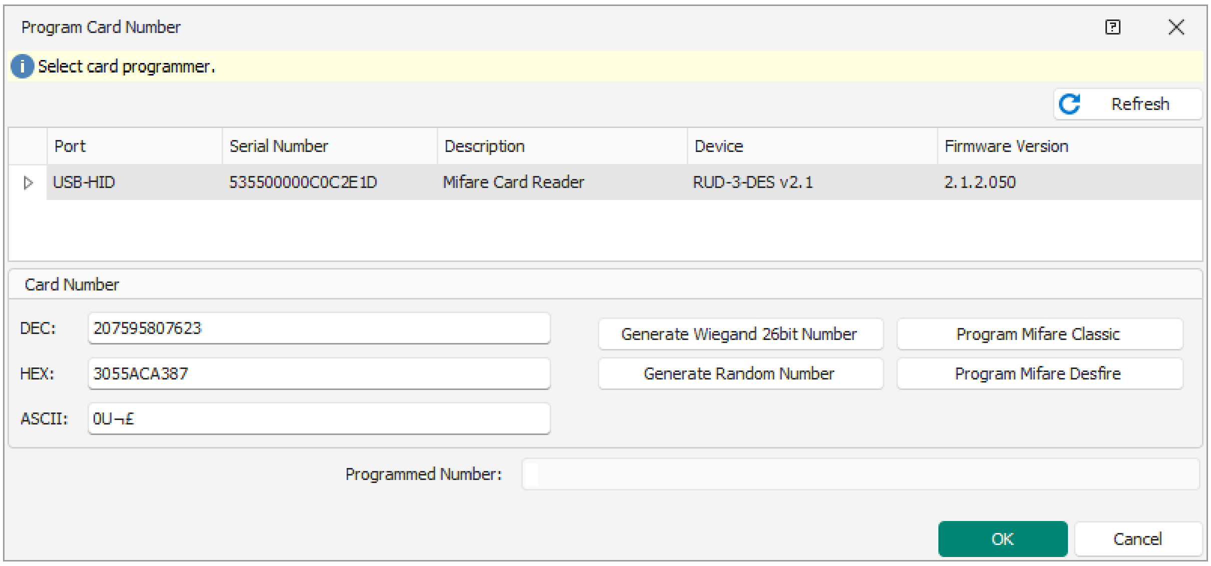
Type: 40 bit proximity card

Factor Value

Value (DEC):

Value (HEX):

- In the newly opened window generate random number or enter your own number in *Card number* area. Select program card button depending on MIFARE card type and read the card at the programmer. Close the window with *OK* button.
- Program remaining cards in the same way, each with their own PCN.



Program Card Number

Select card programmer.

	Port	Serial Number	Description	Device	Firmware Version
▷	USB-HID	535500000C0C2E1D	Mifare Card Reader	RUD-3-DES v2.1	2.1.2.050

Card Number

DEC: 207595807623

HEX: 3055ACA387

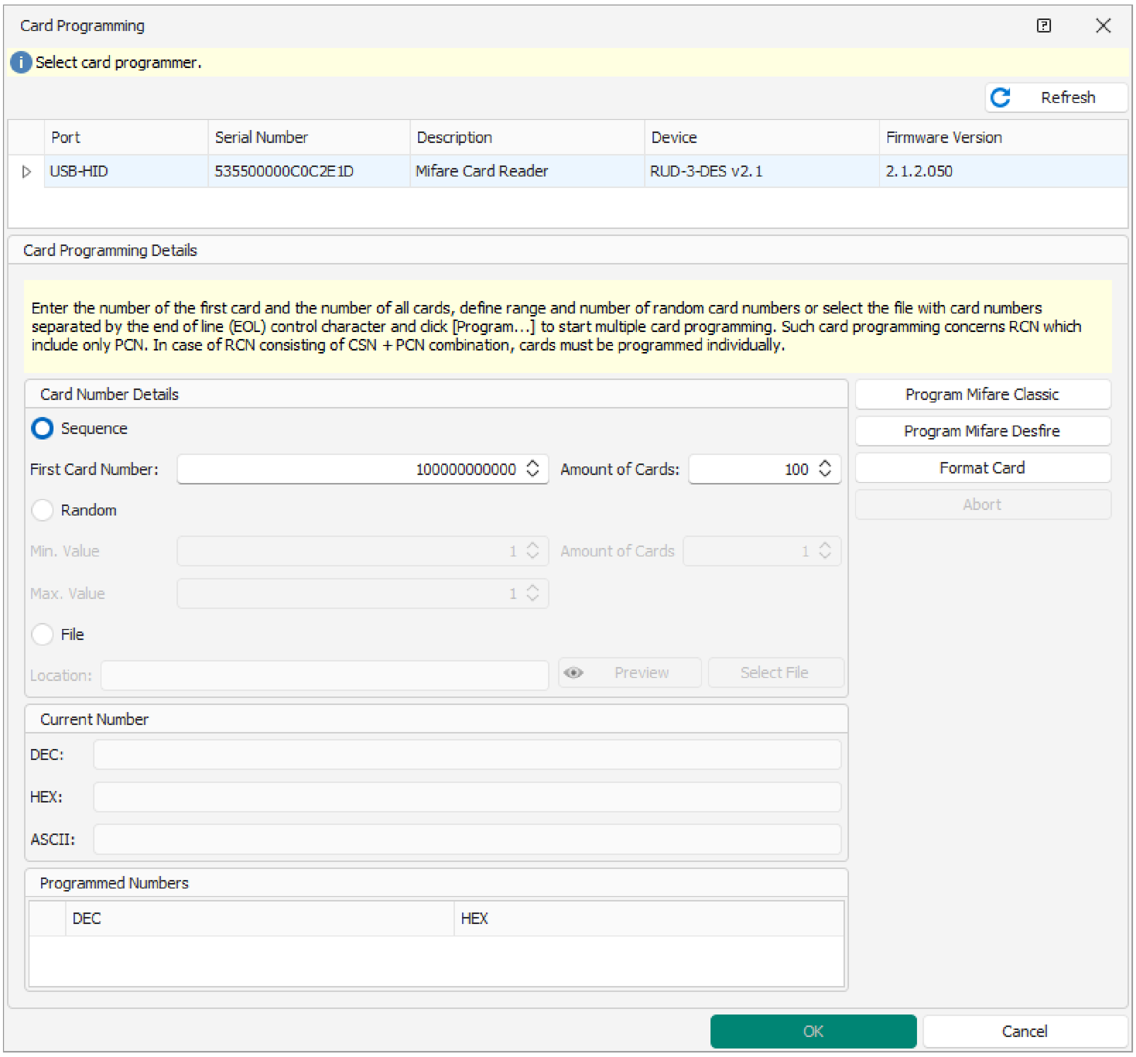
ASCII: 0U¬£

Programmed Number:

PCN serial programming with VISO software:

PCN serial programming is possible only if RCN = PCN. If RCN is configured as sum of CSN and PCN then only earlier mentioned standard programming of individual cards is possible.

- Connect card programmer (e.g. RUD-3-DES, RUD-4-Des) to computer’s USB port. RCN format must configured in the same way for all card programmers and readers in the system.
- Start VISO software, in the top menu select *Configuration* and then *Card Box*.
- In the opened window select *Multiple Program*.
- In the next window it is possible to select sequential or random card number programming as well as indicate a file with card numbers to be programmed.
- Select program card button depending on MIFARE card type and read consecutive cards at the programmer. Close the window with *OK* button and the dialog box will be displayed in order to specify type of Authentication Factors to be added to Card box.



Card Programming

Select card programmer.

	Port	Serial Number	Description	Device	Firmware Version
▷	USB-HID	535500000C0C2E1D	Mifare Card Reader	RUD-3-DES v2.1	2.1.2.050

Card Programming Details

Enter the number of the first card and the number of all cards, define range and number of random card numbers or select the file with card numbers separated by the end of line (EOL) control character and click [Program...] to start multiple card programming. Such card programming concerns RCN which include only PCN. In case of RCN consisting of CSN + PCN combination, cards must be programmed individually.

Card Number Details

● Sequence

First Card Number: 100000000000 Amount of Cards: 100

○ Random

Min. Value 1 Amount of Cards 1

Max. Value 1

○ File

Location:

Current Number

DEC:

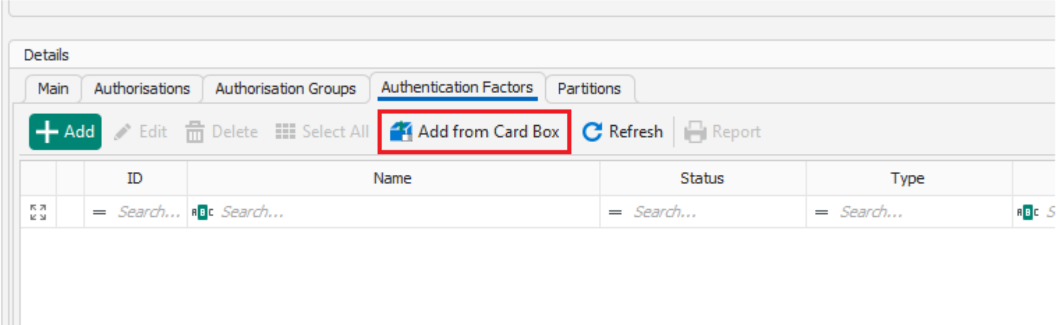
HEX:

ASCII:

Programmed Numbers

	DEC	HEX

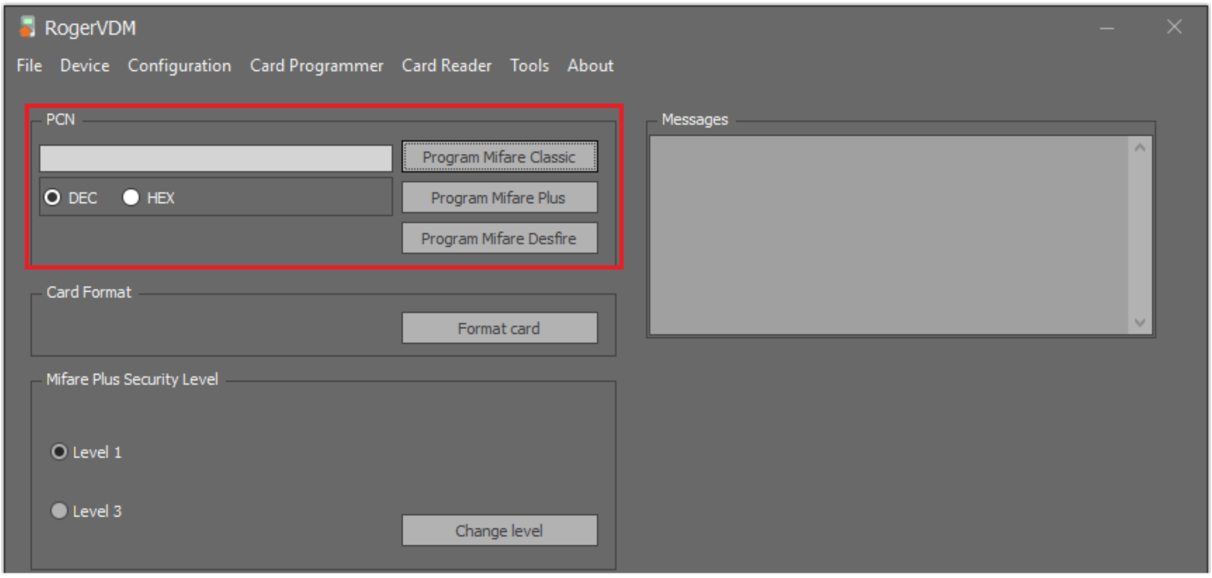
- Authentication Factors for programmed cards are added to Card Box. When users are defined or edited with wizards or manually then these Authentication Factors can be selected and assigned.



PCN programming with RogerVDM:

- Connect card programmer (e.g. RUD-3-DES, RUD-4-Des) to computer’s USB port. RCN format must configured in the same way for all card programmers and readers in the system.
- Establish connection using RogerVDM software in the same way as in case of low level configuration.
- In the top menu of RogerVDM select *Card programming* command.
- In the opened window the card can be formatted (erased) if needed. CSN cannot be erased.

- Enter your own number in *PCN* field and select adequate button to program card with PCN.
- Program remaining cards in the same way, each with their own PCN.
- Programmed cards can be further used to define Authentication Factors for users in the system using VISO software.



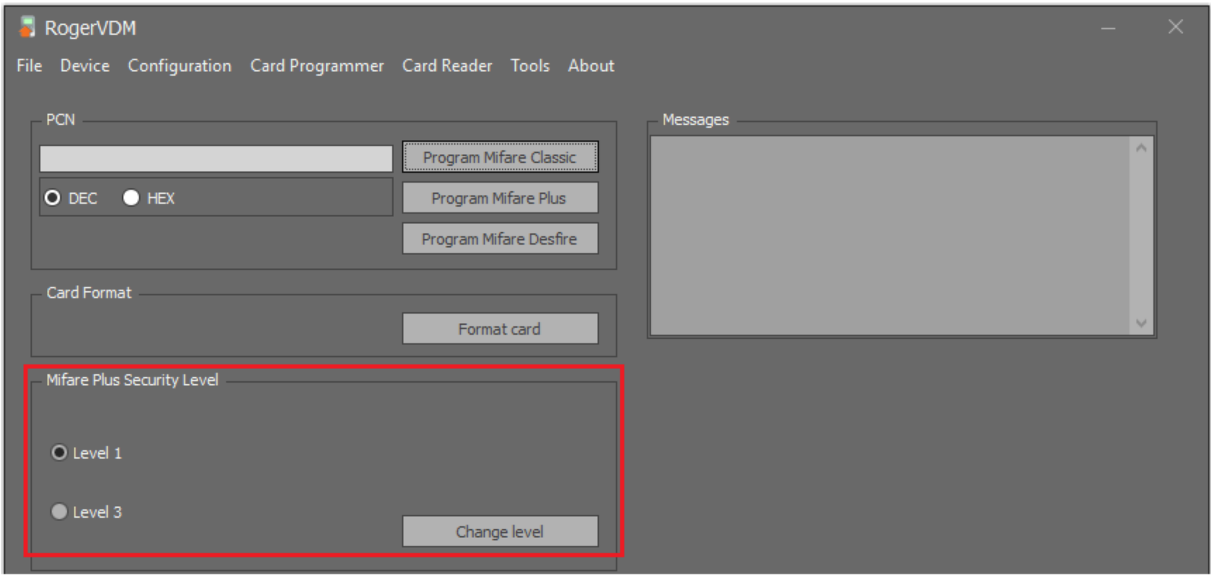
Formatting

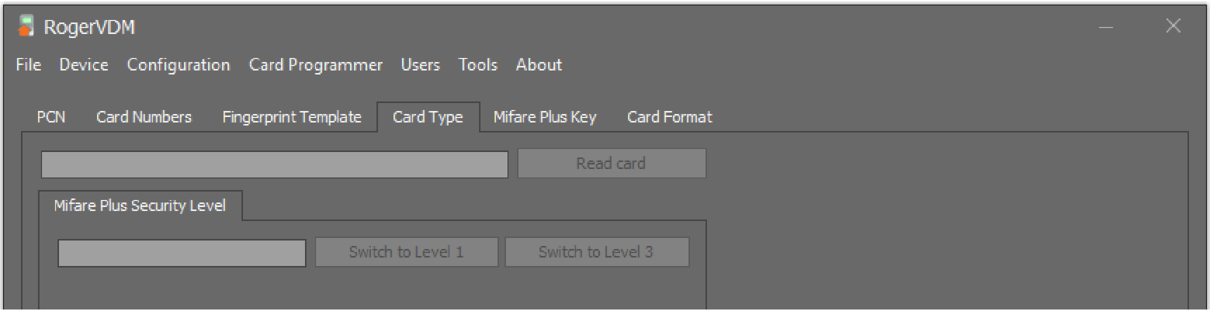
Both RogerVDM and VISO programs enable to format MIFARE cards i.e. erase their memory but in case of:

- MIFARE Clasic/Plus – all sectors which can be accessed by reader (e.g. RUD-3) are formatted based on such parameters as *Key type* and *Key*.
- MIFARE DESFire – the whole card is erased.

Additional notes on MIFARE Plus cards

New MIFARE Plus X cards are configured with security level SL=0 and then it is not possible to program PCN. Security level can be changed with RogerVDM and RFT1000 reader.




RogerVDM
File Device Configuration Card Programmer Users Tools About
PCN Card Numbers Fingerprint Template Card Type Mifare Plus Key Card Format
Read card
Mifare Plus Security Level
Switch to Level 1
Switch to Level 3

Security level can be changed only upward. On the level SL=1, MIFARE X Plus emulates MIFARE Classic card and then its programming is done as if it was MIFARE Classic card. When switched to SL=3 then it can actually be programmed and read in RACS 5 system as MIFARE Plus card enabling its security and functionality to be used in full extent.

Contact:
Roger sp. z o.o. sp.k.
82-400 Sztum
Gościszewo 59
Tel.: +48 55 272 0132
Fax: +48 55 272 0133
Tech. support.: +48 55 267 0126
E-mail: support@roger.pl
Web: www.roger.pl