

Roger Access Control System

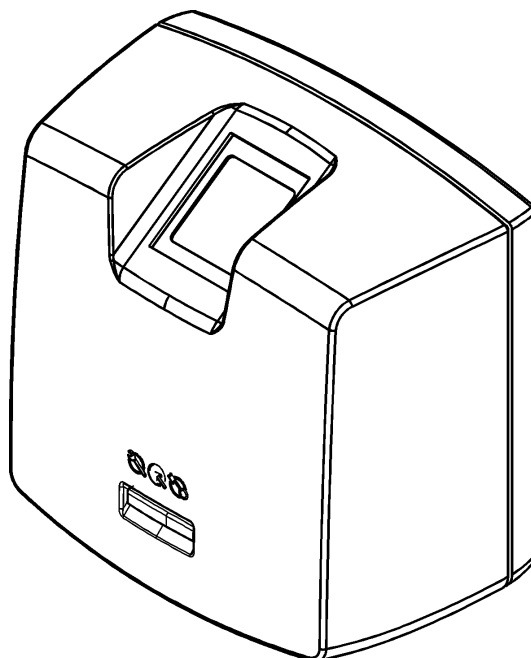
RFT1000 reader in RACS 4

User Manual

Firmware version: 1.2

Hardware version: 1.1

Document version: Rev. H



Contents

1. Introduction	3
2. Description and Specification.....	3
3. Installation	4
3.1 Terminals and connection diagram	4
3.2 LED indicators	8
3.3 Power supply	8
3.4 Inputs	8
3.5 Wall mounting.....	9
3.6 Use/installation guidelines.....	10
4. Configuration.....	10
4.1 Configuration by means of RogerVDM	11
4.1.1 Connection and communication parameters	11
4.1.2 Connection with controller.....	12
4.1.3 Recognition modes	12
4.1.4 Inputs.....	13
4.2 Configuration by means of PR Master software	14
4.2.1 Selection of reader type and recognition mode	14
4.2.2 Connection with RFT1000 reader	15
4.2.3 Users	15
4.2.4 Enrolment of users with fingerprint templates in reader memory (1:N mode)	16
4.2.5 Enrolment of users with fingerprint templates on MIFARE cards (1:1 mode).....	17
4.3 User identification	18
4.4 Card code	19
4.4.1 SSN code programming	19
4.5 Encrypted communication.....	19
4.6 Full memory reset	20
4.7 Firmware update	20
5. Ordering information.....	21
6. Product history	21

1. INTRODUCTION

Note: Factory new RFT1000 reader is uploaded with firmware v1.4 and it cannot be used in RACS 4 system. In order to use RT1000 in RACS 4 system it is necessary to download firmware v1.2 which is available at www.roger.pl and upload it according to section 4.7 below.

This manual contains minimum information that is necessary to properly install and configure RFT1000 readers in RACS 4 access control system. Additional information on RACS 4 system can be found in following documents which are available at www.roger.pl:

- Functional description of PRxx2 series controllers
- PR Master User manual

The application of RFT1000 reader in RACS 5 and third party systems is described in dedicated documents which are available at www.roger.pl.

2. DESCRIPTION AND SPECIFICATION

RFT1000 biometric reader operates as terminal for PR series controller and is equipped with both fingerprint scanner and MIFARE Ultraligh/Classic proximity card reader.

Initial configuration of RFT1000 reader is performed by means of RogerVDM software through Ethernet port, while further configuration and use is performed by PR Master software. The communication between the reader and RogerVDM/PR Master software is encrypted with AES128 CBC standard. Whereas the communication between RFT1000 reader and controller is performed by means of RACS CLK/DTA interface.

The reader can store up to 1900 fingerprint templates. Users can be identified by comparison of their fingerprints with fingerprint templates recorded in reader's memory (1:N mode) or by comparison of their fingerprints with fingerprint templates recorded in MIFARE Classic card memory (1:1 mode).

The reader in RFT1000-ADM version is installed on metal base and it is operated as administrator reader. Its configuration and management is the same as standard RFT1000 device. It is not necessary to connect it to access controller as for fingerprint scanning of users it is just enough to connect the reader to LAN or RS485.

Note: RFT1000 readers do not use or store full fingerprints. Based on the characteristic points of the fingerprint, the reader generates a certain string of characters using a classified algorithm. The string is then used in access control. It is not possible to recreate the actual fingerprint on the basis of this string and the data stored in the reader is understood only by the reader.

Note: PR Master 4.5.6 or newer is recommended for RFT1000 reader.

Table 1. Specification	
Maximum number of users/fingerprint templates	1900
Fingerprint identification modes	1:N mode – fingerprint templates are recorded in reader memory 1:1 mode – fingerprint templates are recorded on MIFARE Classic cards
EER (error rate)	< 0.1%
Identification time 1:1000	< 760ms
Proximity cards	MIFARE Ultralight/Classic
Supply voltage	Nominal 12VDC, min./max. range 10-15VDC
Avg. current consumption	100 mA for 12VDC
Inputs	Two (IN1,IN2) NO inputs, electrically biased to +12V via 15kΩ resistor, triggering level app. 3.5V

Ethernet	10BASE-T 10/100Mb Ethernet communication port
Port RS485	RS485 communication port
Interfaces	RACS CLK/DTA
Tamper	Isolated contact, NC type, 24V/50 mA rated
Environmental class (according to EN 50131-1)	Class I, indoor general conditions, temperature: +5°C to +40°C, relative humidity: 10 to 95% (no condensation)
IP code	IP41
Dimensions H x W x D	85mm x 85mm x 52mm
Weight	160g
Certificates	CE

3. INSTALLATION

3.1 Terminals and connection diagram

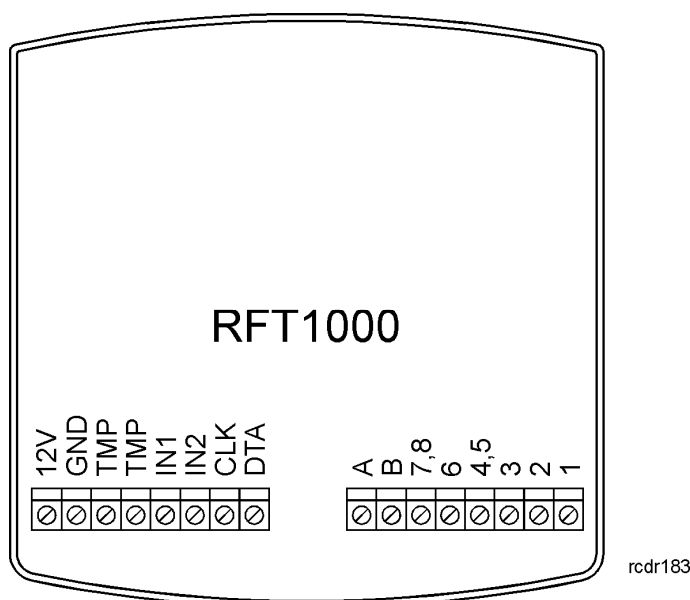


Fig. 1 RFT1000 terminals

Table 2. RFT1000 terminals	
Terminal	Description
12V	Positive power supply contact, 12VDC
GND	Negative power supply contact and reference potential for RS485 communication bus and input lines
TMP	Tamper switch, 24V/50mA
TMP	Tamper switch, 24V/50mA
IN1	IN1 input line
IN2	IN2 input line
CLK	RACS CLK/DTA bus
DTA	RACS CLK/DTA bus
A	RS485 communication bus (line A)

B	RS485 communication bus (line B)
1,2,3,4,5,6,7,8	Ethernet port terminal

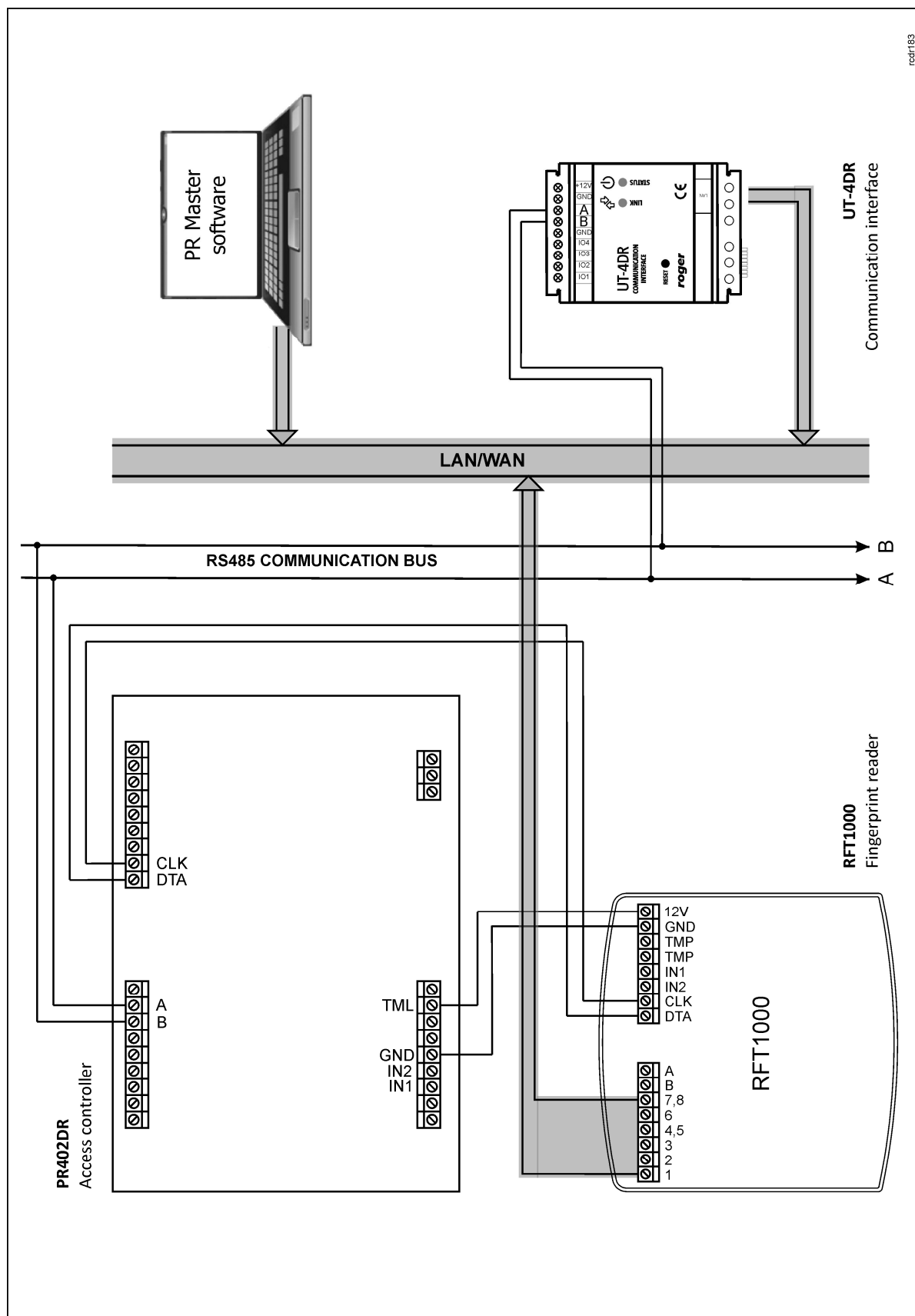


Fig. 2 Connection diagram for RFT1000 reader and PR402DR access controller – configuration through Ethernet (recommended)

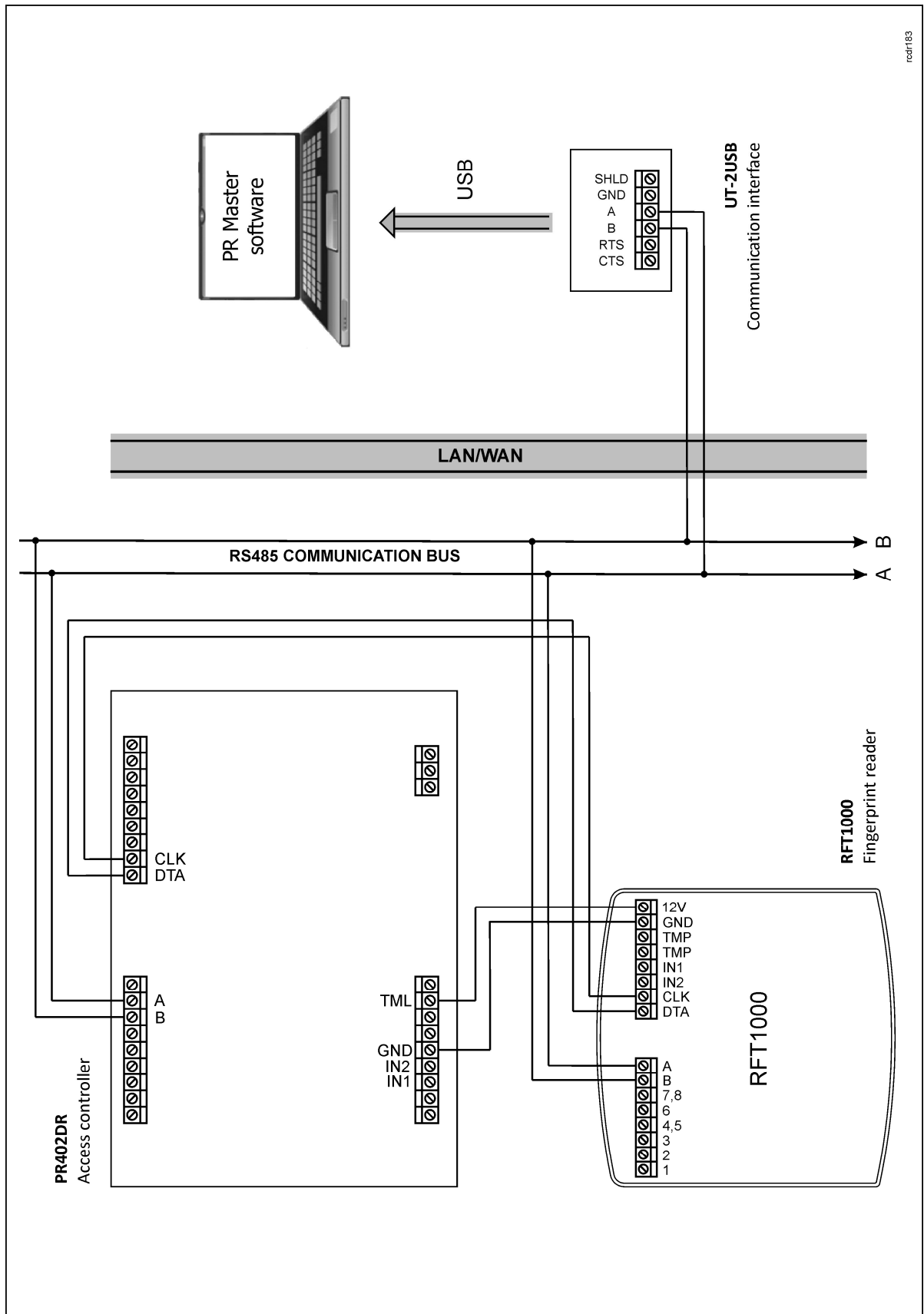





Fig. 3 Connection diagram for RFT1000 reader and PR402DR access controller – configuration through RS485

3.2 LED indicators

RFT1000 reader is equipped with three LED indicators on its enclosure. The indicators operate in the same way as corresponding LED indicators of controller connected to RFT1000.

Table 3. LED indicators			
Symbol	Name	Colour	Description
	STATUS	Red/Green	Armed/Disarmed mode of controller
	OPEN	Green	Door unlocked
	SYSTEM	Orange	Various signalling functions, e.g. microcontroller memory failure, configuration errors, etc.

Note: Synchronic pulsing of LED indicators signifies lost communication with access controller. In case of RFT1000-ADM which does not require connection to controller such pulsing does not signify failure.

3.3 Power supply

RFT1000 reader requires 12 VDC supply voltage. The supply must be connected to +12V terminal and GND terminal. The GND terminal is also reference potential for RS485 bus (if used) and IN1, IN2 input lines.

All devices, which are connected to the same RS485 bus should have common ground (GND). In order to ensure this, all GND terminals of various power supply units in the system must be connected with each other using separate wire. Alternatively, the common negative pole (GND) of the entire system can be earthed, but only in single point.

3.4 Inputs

RFT1000 reader is equipped with two, NO type inputs (IN1 and IN2), which are activated by connection to negative supply pole. By default, inputs are disabled by the they can be configured by means of RogerVDM so they could be used for switching card reader mode. More information on configuration of inputs is given in section 4.1.4 Inputs.

3.5 Wall mounting

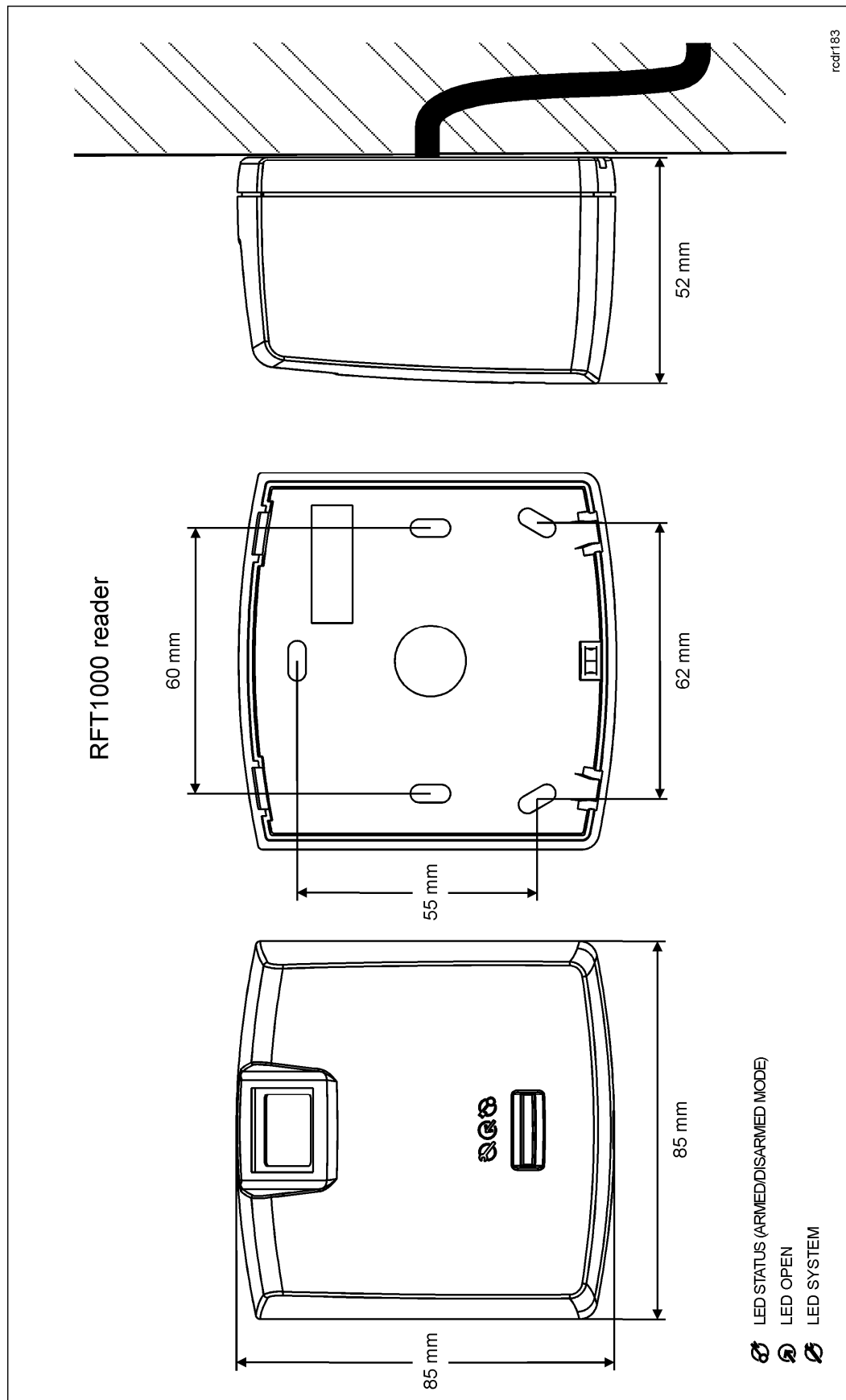


Fig. 4 RFT1000 installation

3.6 Use/installation guidelines

- All electric cables must be connected to devices with disconnected power supply.
- If the range of card reading is significantly lower than specified in technical documentation then consider relocation of reader.
- After installation of RFT1000 reader, remove protector from fingerprint scanner. Otherwise it may hinder fingerprint scanning.
- In case of connection through Ethernet port, twisted pair cable should be uninsulated in the shortest possible distance and wires should remain twisted in the longest possible distance.
- It is required to install proximity card readers in minimal distance of 0.5m from each other.
- In order to ensure correct operation of the reader it is necessary to clean fingerprint scanner regularly by means of wet cloth and mild detergent. Do not clean by means of abrasive materials and strong cleaners like alcohols, solvents, etc. Damages to scanner surface are beyond the scope of warranty.
- RFT1000 reader should be installed in shaded and dry place, far from heat and moisture. It is necessary to avoid dust and abrupt temperature changes. The reader cannot be installed in places exposed to direct sunlight. In the event of exposure of the device to direct sunlight or strong artificial light it may operate improperly.
- In case of communication with RFT1000 reader by means of RS485 bus it is forbidden to apply UT-4 v2.0, UT-4DR or any other Ethernet-RS485 converters.
- It is recommended to use Ethernet interface (instead of RS485) for RFT1000 with 1:N recognition mode and with activated **Admin reader** option
- Proper finger placing for the purpose of fingerprint reading is shown in fig. 5. In case of kids (small fingerprints) it is recommended to verify fingerprint reading prior to installation of RFT1000.

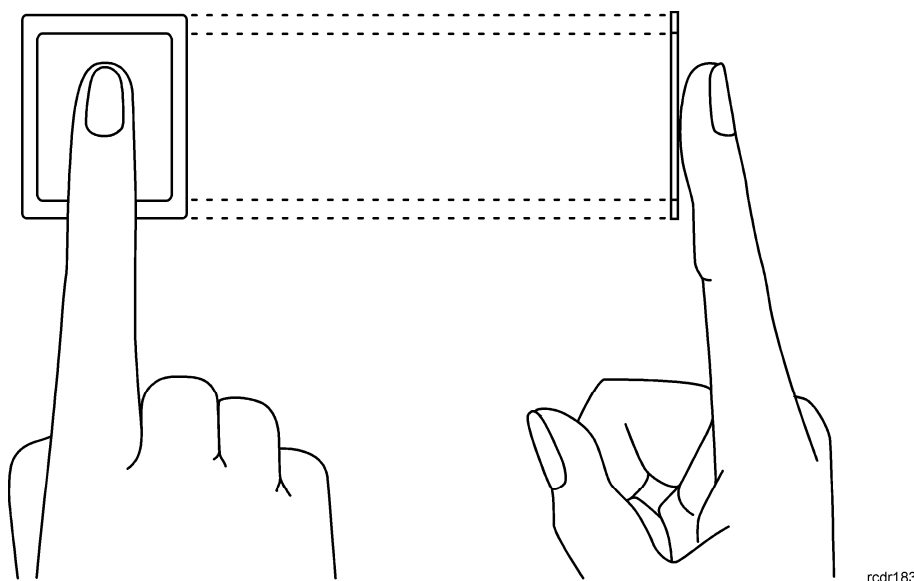


Fig. 5 Proper placing of finger on optical scanner

4. CONFIGURATION

The configuration of RFT1000 reader to be used in RACS 4 system consists in:

1. Connection of the reader to network through Ethernet port according to fig. 2. or through RS485 port according to fig. 3. By default, RFT1000 is configured for Ethernet communication.
2. Installation of RogerVDM software, establishing connection with the reader and performing preliminary setup including reader's communication password.
3. Connection of RFT1000 to controller by means of RACS CLK/DTA interface according to fig. 2.
4. Installation of PR Master software and establishing connection with the reader.

5. In case of 1:N recognition mode, enrolment of users including their fingerprint templates and card numbers by means of PR Master software.
6. In case of 1:1 recognition mode, enrolment of users including their card numbers and then formatting their MIFARE Classic cards and recording fingerprint templates by means of PR Master software.
7. Sending the configuration to the reader by means of PR Master software.

4.1 Configuration by means of RogerVDM

RogerVDM software is used for initial configuration of RFT1000 reader. Further configuration including enrolment of users is performed by means of PR Master software.

4.1.1 Connection and communication parameters

In order to connect and configure RFT1000 reader it is necessary to know its communication parameters. Factory default settings are as follows:

- IP address = 192.168.0.70
- Subnet mask = 255.255.255.0
- Port = 13544
- Communication is encrypted with default (empty) password

It is assumed that mentioned above parameters will be changed in particular access control installation, specifically IP address, port and communication password. These parameters can be modified with RogerVDM software, which is available for download at www.roger.pl.

Note: In order to connect with reader in local area network (LAN), the computer with RogerVDM software must be in the same subnet. In case of RFT1000 with default IP address, the IP address of computer should be 192.168.0.xxx.

Procedure for establishing connection with factory new reader

1. Connect the reader to computer by means of Ethernet port.
2. Install and start RogerVDM software.
3. In the top menu of RogerVDM select **Device** and then **New**.
4. In the newly opened window (see fig.6) select **RFT1000 v1.0** device, firmware version **1.2** and then **Ethernet** communication channel.
5. IP address and port of RFT1000 reader is automatically detected by RogerVDM software if the reader and PC with RogerVDM are in the same subnet and communication between them is not blocked. Default IP address of the reader is 192.168.0.70 and port is 13544, while communication passwords is empty.
6. Select **Connect** button.

After establishing the connection it is possible to modify communication parameters both for Ethernet and RS485 communication in the newly opened window, which can be accessed by selecting the option **Configuration** in the top menu. In the area **General settings** (see fig. 7) enter your settings and then upload the configuration to the reader by means of **Send to device** button.

Select Device

Device

Device: RFT1000 v1.0

Firmware version: v1.2

Communication channel: Ethernet

Connection parameters

IP Address: 192.168.0.70:13544

Communication password:

Connection info

Communication channel: Ethernet

Device: RFT1000 v1.0 fv1.2

Connect

Fig. 6 Connection with RogerVDM software

4.1.2 Connection with controller

RFT1000 reader can communicate with PR series controller by means RACS CLK/DTA bus. After connection according to fig. 2, RFT1000 reader must be configured for communication through RACS CLK/DTA bus, while PR series controllers by default are configured for such communication.

In order to configure RFT1000 in RogerVDM software select the option **Configuration** and in the area **General Settings**, in the field **Output format** select one of following options:

- [000] RACS ID=0 if RFT1000 reader is to operate with ID =0 address
- [001] RACS ID=1 if RFT1000 reader is to operate with ID =1 address
- [002] RACS ID=2 or [003] RACS ID=3 if RFT1000 reader is to operate as additional terminal in High Security mode (more information on High Security mode is given in functional manual of PRxx2 series controllers).

4.1.3 Recognition modes

In case of RFT1000 it is necessary to select one of following recognition modes:

- 1:N mode (templates in reader's memory) – in this mode, fingerprint templates are recorded in memory (database) of RFT1000 reader. Users are identified by comparison of their fingerprints with fingerprint templates recorded in reader memory.
- 1:1 mode (templates on Mifare cards) – in this mode, fingerprint templates are recorded only on Mifare cards and not in reader's memory. Users are identified by comparison of their fingerprints with fingerprint templates recorded in memory of Mifare card.

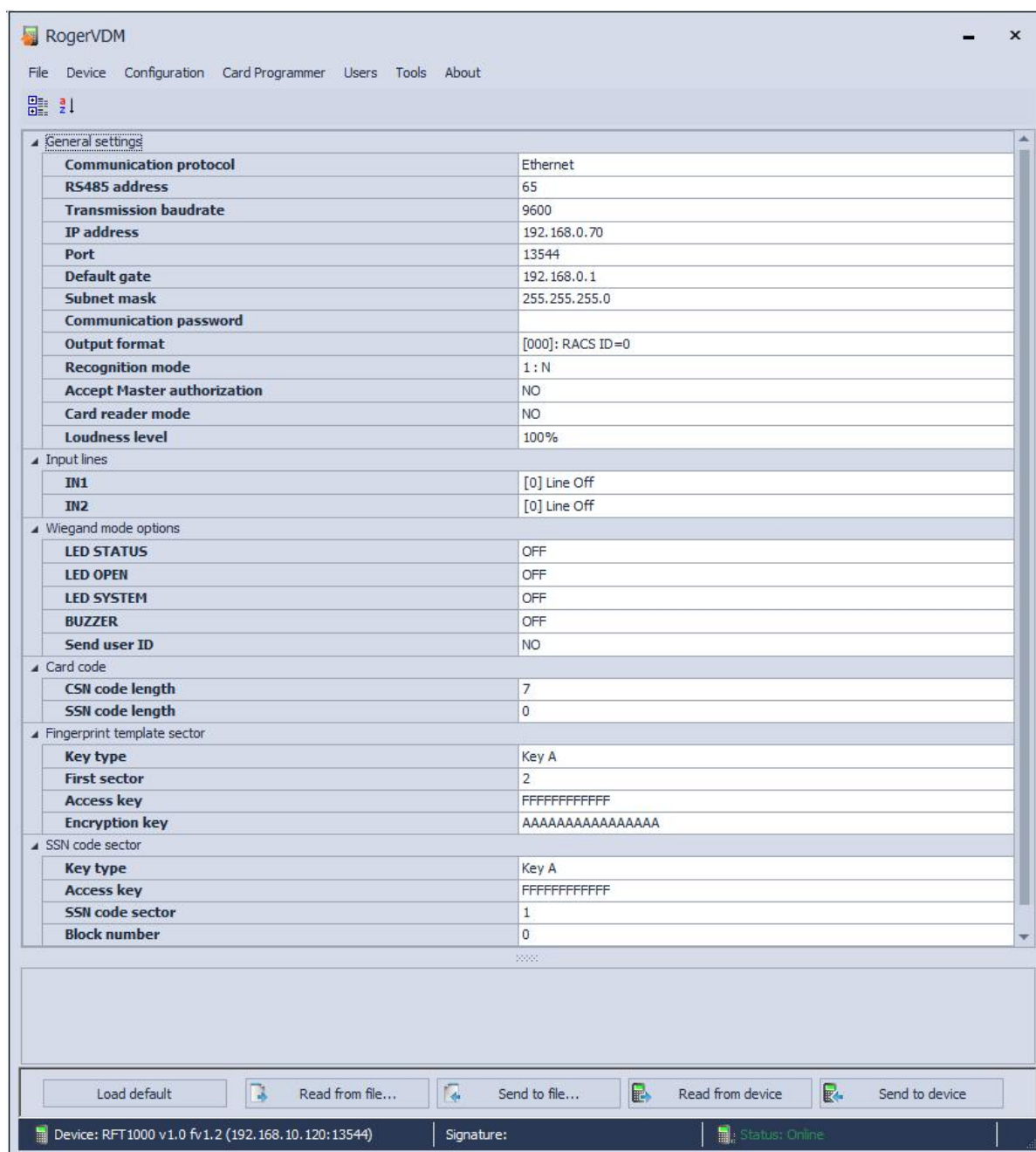


Fig. 7 RFT1000 configuration in RogerVDM software

4.1.4 Inputs

RogerVDM software enables configuration of RFT1000 inputs. Related options are available in the area **Input lines**, which can be displayed by means of the command **Configuration** in the top menu of RogerVDM software (see fig. 7). When RFT1000 reader is installed in RACS 4 system, only the function **[5]: Card Reader Mode** is applicable. Other available functions are used beyond RACS systems.

In general, input functions of Roger devices depending on assigned functions can be momentary or constant type. Therefore device may detect only activation of input (momentary type) or activation and deactivation of input (constant type).

Table 3. Input functions			
No.	Function	Type	Description
[0]	None	-	Input line is not used.

[1]	LED STATUS	Constant	Not applicable in RACS 4
[2]	LED OPEN	Constant	Not applicable in RACS 4
[3]	LED SYSTEM	Constant	Not applicable in RACS 4
[4]	BUZZER	Constant	Not applicable in RACS 4
[5]	Card Reader Mode	Constant	<p>Functioning of input line with function [5] depends on selected recognition mode. More information on recognition mode is given in section 4.2.1 Selection of reader type and recognition mode.</p> <p>In case of 1:N recognition mode:</p> <ul style="list-style-type: none"> • when the input is activated then RFT1000 can scan fingerprints and read proximity cards • when the input is deactivated then RFT1000 can only scan fingerprints <p>In case of 1:1 recognition mode:</p> <ul style="list-style-type: none"> • when the input is activated then fingerprint scanner is off and user can identify only by means of proximity card • when the input is deactivated then RFT1000 requires proximity card and then when LED OPEN pulsates also fingerprint scan

4.2 Configuration by means of PR Master software

4.2.1 Selection of reader type and recognition mode

After installation of PR Master software and initial configuration of RFT1000 reader by means of RogerVDM, it can be further used in RACS 4 system. Therefore in the top menu of PR Master select the option **Tools**, then **Options** and **Fingerprint readers** tab. In the window shown in fig. 8, select the type of installed fingerprint readers and in case of RFT1000 also recognition mode. Selected recognition mode must be the same as previously selected by means of RogerVDM software – see section 4.1.3 Recognition modes. Each modification of recognition mode in PR Master software requires also respective modification of recognition mode by means of RogerVDM software.

Note: In RACS 4 system, both older fingerprint readers (F7, F8, F10, F11) and newer fingerprint readers (RFT1000) cannot be used simultaneously.

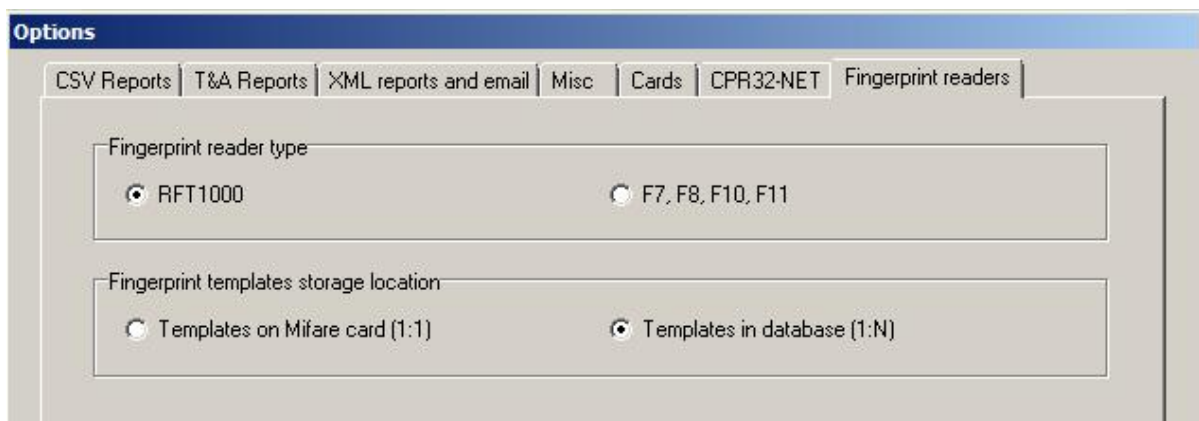


Fig. 8 Selection of fingerprint readers type in PR Master

4.2.2 Connection with RFT1000 reader

In order to connect with RFT1000, select the option **Fingerprint readers** in the main window of PR Master software and then click the button **Add**. In the window shown in fig. 9, select RFT1000 reader and then select communication channel: Ethernet or RS485. The channel must be the same as previously selected in RogerVDM software and it must be in accordance with applied cabling – see fig. 2 (Ethernet) or fig. 3 (RS485).

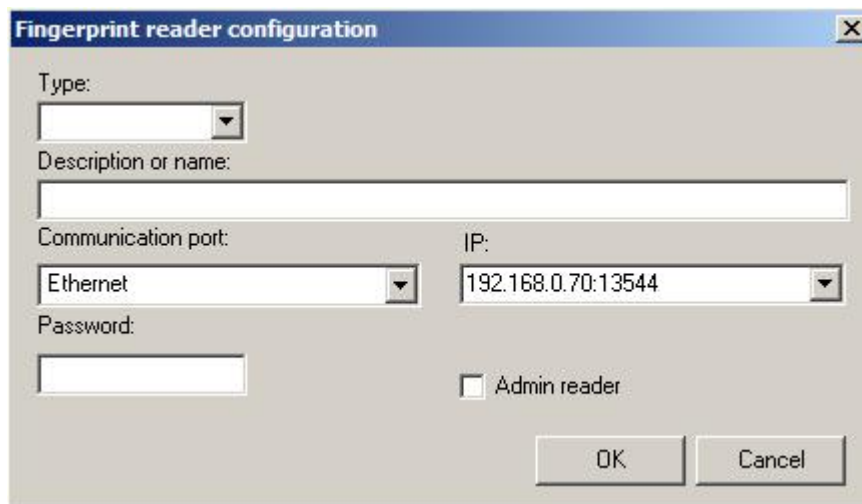


Fig. 9 Connection with RFT1000 in PR Master software

If Ethernet communication channel is selected then RFT1000 IP address and port should be detected automatically by PR Master software if the reader and PC with RogerVDM are in the same subnet and communication between them is not blocked. Default communication password is empty. More information on encrypted communication with RFT1000 is given in section

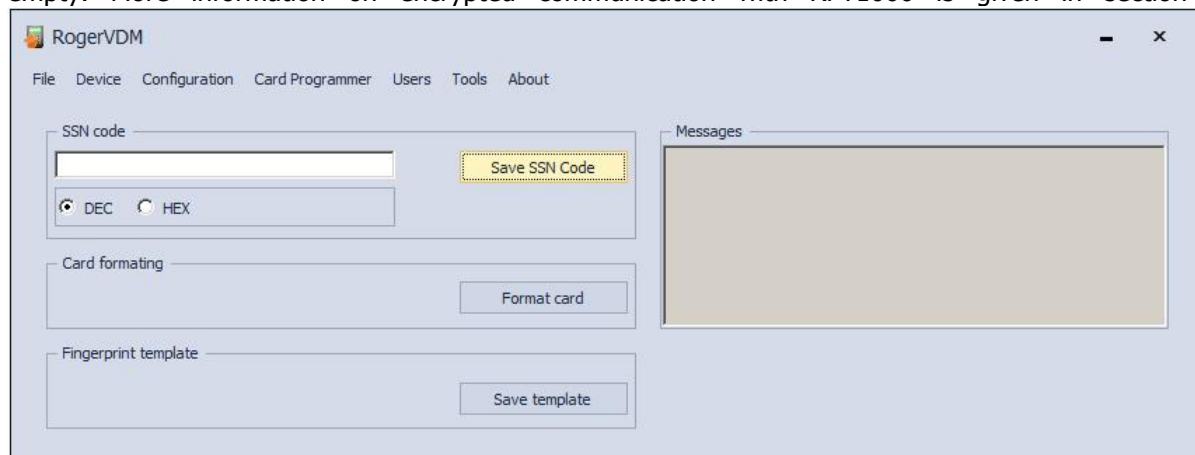


Fig. 12 SSN code definition

4.5 Encrypted communication. When adding RFT1000 readers in PR Master software it is necessary to indicate at least one of readers as administrator reader by means of the option **Admin reader**.

4.2.3 Users

Users enrolment for both recognition modes and management of access rights are performed by means of PR Master software. Users can be enrolled by means of **Users** option or **Quick user update** option in the main window of PR Master. In both cases, user enrolment procedure is the same. In case of **Users** option, after user enrolment it is necessary to upload configuration data to RACS 4 devices by means of button **Update system now**.

After selection of **Users** or **Quick user update** options, in the newly opened window select the button **Add**. In RACS 4 there are several types of users but NORMAL user is used most often. In

the next window, in the tab **General** enter first/last name of user and select Group. In the tab **Identification** (see fig. 10), card number, PIN and/or fingerprint templates can be assigned to the user.

Note: The button **Clear** erases fingerprint templates of particular user only from PR Master database. In order to remove fingerprint templates from reader's memory (if such templates were previously uploaded to the reader at all) it is necessary to upload new configuration to the reader.

Note: More information on user enrolment and access rights is given in such documents as: PRxx2 series controllers, Functional description and programming guide; PR Master User manual.

Selection of the button **Scan** results in opening the window (see fig. 11), which enables scanning and assigning of fingerprint templates to particular user.

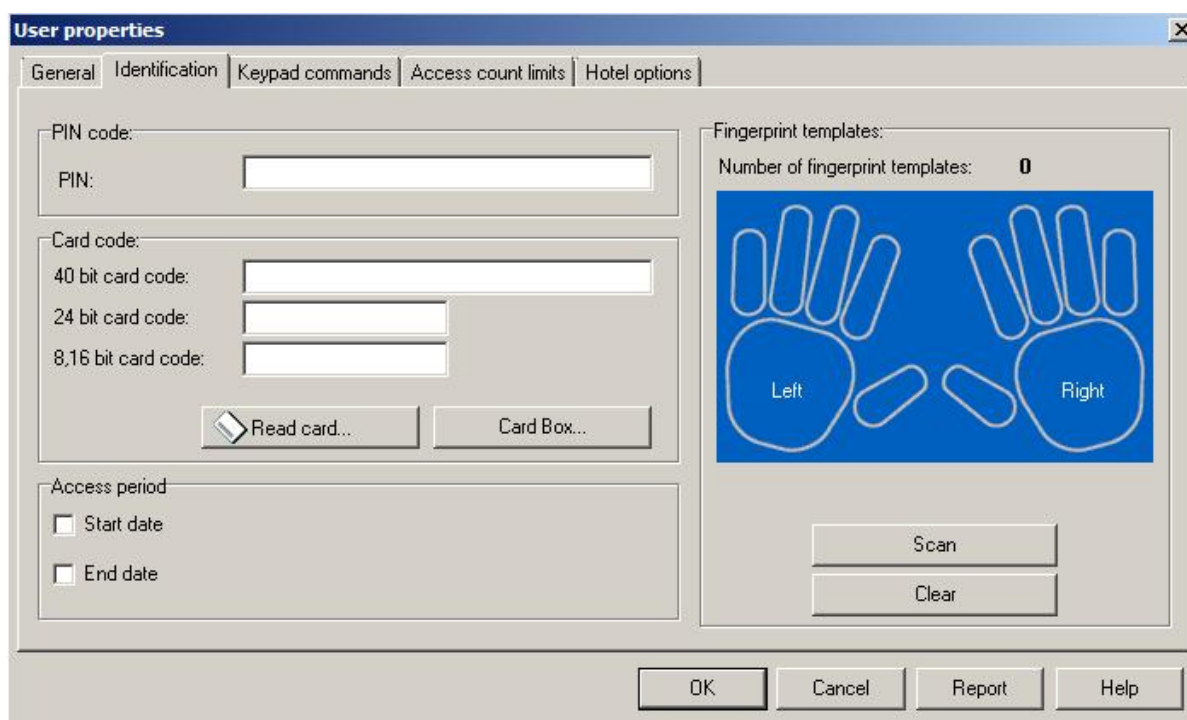


Fig. 10 Identification tab in user properties

4.2.4 Enrolment of users with fingerprint templates in reader memory (1:N mode)

Enrolment of user in this mode requires selection of **Scan** button in the window shown in fig. 10. In the newly opened window select the button **Configure** in order to upload data to RFT1000 administrator reader and then select the button **Read**. The memory of such reader shall be overwritten for the period of fingerprint scanning. The idea of administrator reader was applied in order to avoid erroneous assignment of the same fingerprints to different users. It is not required to use dedicated RFT1000 reader as administrator reader. Any RFT1000 available in RACS 4 can be used as administrator reader. The memory of such reader shall be overwritten for the period of fingerprint scanning but after upload of configuration data to RACS 4 system, its settings shall be restored.

In the window shown in fig. 11 fingers for scanning can be selected by means of numeric buttons. When selected, scanning procedure is started and it is necessary to follow displayed messages. After fingerprint scanning, close the window by means of **OK** button. Then in the window shown in fig. 10 user's card number can be specified. Card number can be entered manually in the field **40bit card code** or it can be read by available MIFARE reader in the window opened by means of **Read card...** button. Depending on RFT1000 configuration, built-in proximity reader can be activated or deactivated. Therefore card number can be read by means of such devices as PRTxxMF series reader (if available), RUD-3 reader (if available) or RFT1000 MIFARE reader (when

activated). Conditions and methods for activation of MIFARE proximity card reader in RFT1000 are given in section 4.3 User identification.

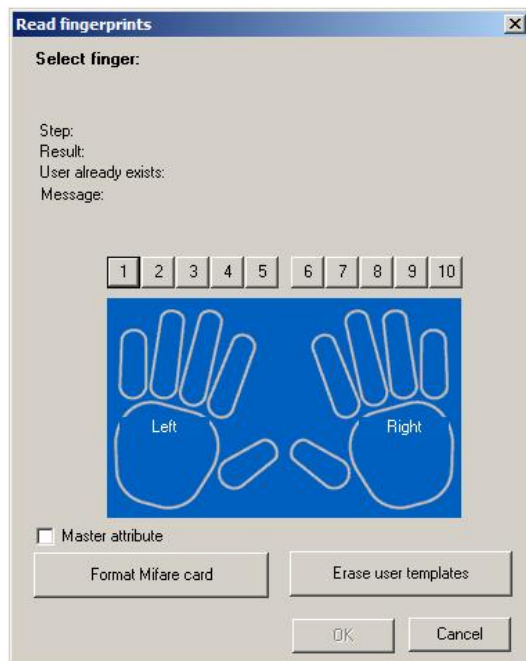


Fig. 11 Fingerprint scanning window in PR Master

4.2.5 Enrolment of users with fingerprint templates on MIFARE cards (1:1 mode)

Enrolment of user in this mode requires selection of **Scan** button in the window shown in fig. 10 and then selection of RFT1000 reader to be used in fingerprint scanning.

Procedure for recording of fingerprint templates on MIFARE card:

1. It is recommended to format (erase) card memory by means of the button **Format Mifare card** (see fig. 11).
2. Select one of numeric buttons in order to start scanning procedure. Successive steps of the procedure are indicated by means of displayed messages.
3. After closing the window with **OK** button it is necessary to assign MIFARE card number to the user in the field **40 bit card code** (see fig. 10)
4. Card number can be entered manually or read by means of RFT1000 MIFARE card reader.
5. In order to use built-in MIFARE card reader, click the button **Read card...** (see fig. 10), select controller with RFT1000 reader, place card in vicinity of RFT1000 and when LED OPEN (green) flashes scan fingerprint, which is already recorded on card.

Note: MIFARE cards have different capacities. MIFARE Classic 1k cards can store 1 fingerprint template, while MIFARE Classic 4k card can store up to 7 fingerprint templates. MIFARE Ultralight cards do not have enough memory to store any fingerprint template.

Any user can have Master attribute. When the option **Master attribute** is activated for particular user (see fig. 11) then such user will not be obliged to scan his fingerprint at all RFT1000 readers with activated option **Accept Master authorization** (see fig. 7). Such user shall be identified only by means of his MIFARE proximity card number.

It is also possible to define sectors in MIFARE Classic memory cards, where fingerprints templates are to be recorded. Related options are available in the configuration window of RogerVDM software in the area **Fingerprint template sector** (see fig. 7):

- **Key type** – enables selection of two available access keys for card memory sectors
- **First sector** – defines first sector of card memory, where fingerprint templates are to be recorded
- **Access key** – defines access key for card memory sectors

- **Encryption key** – defines key for additional securing of data stored in memory card sectors

Note: Options in the area **Fingerprint template sector** define both the method for recording fingerprint templates during card programming and method for card reading by particular RFT1000 reader during user identification. Therefore it is necessary to ensure that in both cases i.e. card programming and user identification, mentioned settings are the same.

Note: In case of RFT1000 with firmware 1.2 or newer, default **First sector** was changed to 2 and default **Encryption key** was changed to AAAAAAAAAAAAAAAAAA. This must be taken into account by administrators who want to upgrade their RFT1000 readers with newer firmware and want to use previously configured proximity cards in 1:1 recognition mode.

4.3 User identification

User identification by RFT1000 reader depends on selected recognition mode (see section 4.2.1), input with function **[5]: Card Reader Mode** (see section 4.1.3) and option **Card reader mode** (see fig. 7). Input **[5]** is used for dynamic switching of user identification method in such way that it depends on input state. More information on application of the input **[5]** is given in table 4 below. The option **Card Reader Mode** is applicable only for 1:N recognition mode and it enables permanent activation of card reader in RFT1000. When this option is selected then user can identify by means of card or fingerprint templates as needed.

Options and functions of RogerVDM enable detailed and variant configuration of user identification method. But there can be distinguished following most often applied settings:

- 1:N recognition mode, **[5]** input is not used, **Card Reader Mode** option inactive – user is identified only by fingerprint templates recorded in RFT1000 memory
- 1:N recognition mode, **[5]** input is not used, **Card Reader Mode** option is active – user can identify by means of fingerprint template recorded in RFT1000 memory or by means of his MIFARE card as needed
- 1:1 recognition mode, **[5]** input is not used, **Card Reader Mode** option is inactive – user must at first use his MIFARE card with his fingerprint templates and then he must place his finger on RFT1000 scanner

Table 4. User identification by RFT1000 with [5] input.

Recognition mode	Card Reader Mode	User identification
1:N	Input with the function [5] deactivated	Place finger on RFT1000 scanner.
1:N	Input with the function [5] activated	Place finger on RFT1000 scanner or read proximity card.
1:1	Input with the function [5] deactivated	Place your MIFARE proximity card in vicinity of RFT1000 reader and when LED OPEN (green) flashes, place your finger on RFT1000 scanner. User's card does not have to be in vicinity of reader when LED OPEN pulsates. Users with Master attribute can use their cards and they do not have to scan their fingerprints in order to get access.
1:1	Input with the function [5] activated	Read proximity card.

4.4 Card code

MIFARE Classic and MIFARE Ultralight cards have their read-only serial numbers called CSN and memory, where administrator defined number called SSN can be stored. Optional SSN code provides additional security as it can be saved in administrator defined sector and it can be protected with access code against unauthorized reading. RogerVDM software enables defining of SSN code and recording it to any available sector of MIFARE card memory. RFT1000 reader can identify particular card (user) by means of CSN code, SSN code or combination of both but the total number identified in RACS 4 system is limited to 5 bytes. Options related to reading of CSN and SSN codes are available in **Card code** area of reader configuration window (see fig. 7)

Example:

Default settings of RFT1000 reader in Card code area is as follows: CSN code length = 7, SSN code length = 0. In case of such settings, the RFT1000 reads 7 bytes of CSN code only. In case of exemplary settings: CSN code length = 3, SSN code length = 2, RFT1000 reader during card identification would read code consisting of 3 bytes of CSN code and 2 bytes of SSN code.

4.4.1 SSN code programming

SSN code as opposite to CSN code of MIFARE card can be defined by administrator. SSN Code as well as its sector in memory and method for recording can be indicated by administrator. SSN code can be defined and recorded by means of RogerVDM options, which are available in the area **SSN code** in the **Card programmer** window (see fig. 12). After selection of **Save SSN code** button it is necessary to hold the card in vicinity of RFT1000 reader. The code can be entered in decimal or hexadecimal format. Location and recording method can be defined by means of options, which are available in the area **SSN code sector** (see fig. 7):

- **Key type** – enables selection of two available access keys for card memory sectors
- **Access key** – defines access key for card memory sectors
- **Sector** – defines sector of card memory, where SSN code is to be recorded
- **Block number** – defines block number of card memory where SSN code is to be recorded

Note: Options in the area **SSN code sector** define both the method for SSN code recording during card programming and method for SSN code reading by particular RFT1000 reader during user identification. Therefore it is necessary to ensure that in both cases i.e. card programming and user identification, mentioned settings are the same.

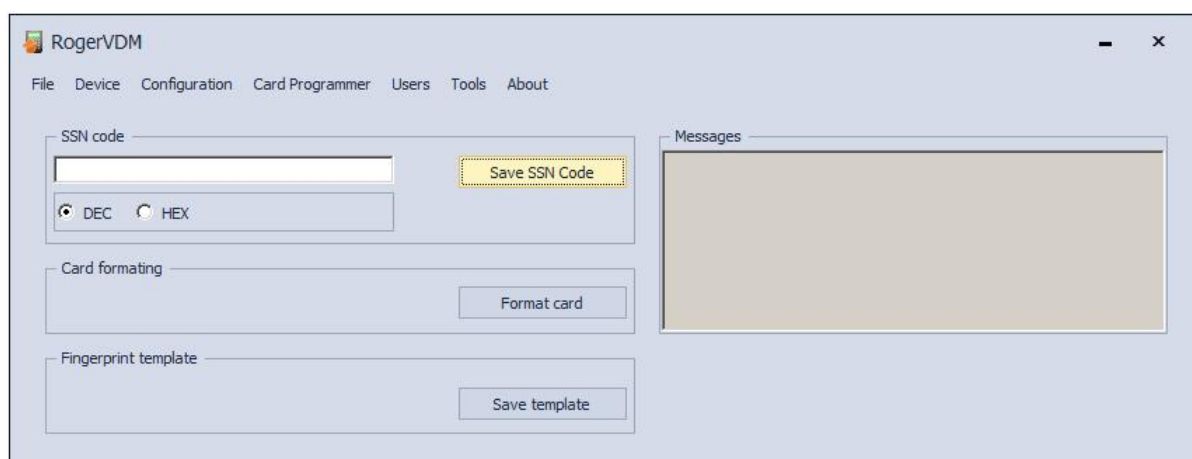


Fig. 12 SSN code definition

4.5 Encrypted communication

The communication with RFT1000 reader both in case of Ethernet and RS485 port can be encrypted with AES128 CBC standard. By default, encryption is conducted with empty communication password. Administrator can define his own communication password (max. 16 digits) in reader configuration window in the field **Communication password** (see fig. 7).

Such password must be then entered when establishing connection with the reader by means of RogerVDM (see fig. 6) and when establishing connection with reader by means of PR Master (see fig. 9).

4.6 Full memory reset

Full memory reset erases current settings, including users data base and restores factory default settings. Reset method must be selected depending on target communication method with the reader (Ethernet or RS485).

Reset procedure (communication channel – Ethernet):

1. Switch off power supply to RFT1000.
2. Remove connections to CLK and IN2 terminals.
3. Connect CLK terminal with IN2 terminal.
4. Switch on power supply to RFT1000. The reader shall generate continuous acoustic signal.
5. Disconnect CLK and IN2 terminals.

Communication parameters after reset:

- IP address = 192.168.0.70
- Subnet mask = 255.255.255.0
- Port = 13544
- Communication is encrypted with default (empty) password

Reset procedure (communication channel – RS485)

1. Switch off power supply to RFT1000.
2. Remove connections to CLK and IN1 terminals.
3. Connect CLK terminal with IN1 terminal.
4. Switch on power supply to RFT1000. The reader shall generate continuous acoustic signal.
5. Disconnect CLK and IN1 terminals.

Communication parameters after reset:

- RS485 address= 65
- Transmission baud rate = 9600
- Communication is encrypted with default (empty) password

Note: Because of relatively high current consumption of RFT1000, it cannot be supplied by means of RUD-1 communication interface and use of external power supply unit is necessary. In case of connection by means of RS485 port it is also necessary to connect GND of power supply unit with GND of RS485 communication bus.

4.7 Firmware update

Firmware update is performed by means of RogerVDM software and the recommended communication channel is Ethernet port. In order to update the firmware:

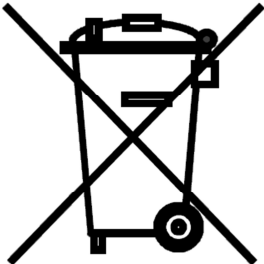

1. Establish connection with your RFT1000 using RogerVDM software.
2. Select the command **File** in the top menu of RogerVDM software and then select **Send Configuration to File** in order to export current settings of your RFT1000.
3. Select the command **Tools** in the top menu of RogerVDM software and then select **Update Firmware**.
4. In the opened window select RFT1000 firmware file (*.frg extension) by means of the button **Select file**.
5. Select the button **Update** in order to upload the firmware to RFT1000.
6. After firmware upload make full reset according to section 4.6.
7. Establish connection with RFT1000 using RogerVDM software.
8. Select the command **File** in the top menu of RogerVDM software and then **Read Configuration from File** in order to import previous settings.

5. ORDERING INFORMATION

Table 5 Ordering information	
Product	Description
RFT1000	Fingerprint and MIFARE Ultralight/Classic proximity card reader.
MFC-2	13.56 MHz MIFARE Classic ISO size thin PVC card, 1k bytes memory.
MFC-3	13.56 MHz MIFARE Classic ISO size thin PVC card, 4k bytes memory.

6. PRODUCT HISTORY

Table 6 Product history		
Product version	Released	Description
1.0	06/2013	The first commercial version of the product
1.1	12/2013	Built-in antenna modifications

 	<p>This symbol placed on a product or packaging indicates that the product should not be disposed of with other wastes as this may have a negative impact on the environment and health. The user is obliged to deliver equipment to the designated collection points of electric and electronic waste. For detailed information on recycling, contact your local authorities, waste disposal company or point of purchase. Separate collection and recycling of this type of waste contributes to the protection of the natural resources and is safe to health and the environment. Weight of the equipment is specified in the document.</p>
--	---

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