EPSO 2

Communication Protocol

Firmware v2.29

Introduction

The EPSO 2 protocol is a set of communication functions used to control access reader (called Terminal) through a serial interface. This protocol has been designed to allow for direct control of device's hardware through external commands called "functions".
The access unit operating on EPSO 2 protocol act as pure "terminal" what means it strictly follows commands received from a host unit (PC or another controller). The software developer or system integrator must incorporate EPSO 2 protocol into the host device software/firmware to communicate with the device.

The EPSO 2 protocol is available in multiple Roger access products including:

- PRT-EM series readers (RS232 serial interface, EM 125 KHz cards)
- PRT-MF series readers (RS232 serial interface, Mifare cards)
- PR80 series readers (RS485 serial interface, EM 125 KHz cards)

All, listed above devices can work in various (selectable) operation modes, one of them is EPSO 2 protocol. In order to prepare the reader for work on EPSO 2 protocol it must be properly configured using either manual method (**Memory Reset**) or from PC using RARC program.

Optionally, is possible to program the unit with special version of firmware which will make device preconfigured to EPSO 2 protocol only – in this case reader will not require any prior configuration procedures (i.e. it will solely work on EPSO 2 protocol). This special firmware is marked by an extra letter "E" which is added on the first position of the firmware name. For instance, if the standard device's firmware is marked as PR80H then the EPR80H indicates firmware version which is limited to EPSO 2 Protocol operation only.

Host and Terminal

The EPSO 2 protocol defines how two devices can exchange data. The unit which initializes the communication and sends commands is called **Host** while the unit which responses the commands is called **Terminal**. In practice, the Host is a PC or special microprocessor based device (controller) which uses EPSO 2 protocol. Terminal is a PRT-EM, PRT-MF or PR80 series proximity reader configured (or programmed) to work on EPSO 2 protocol. The commands and the responses have a form of byte series (frames) which are described in this document.

External Reader

Regardless fact that some access terminals running on EPSO 2 are equipped with CLK/DTA lines it is not possible to connect additional reader to main access terminal.

Configuration Register

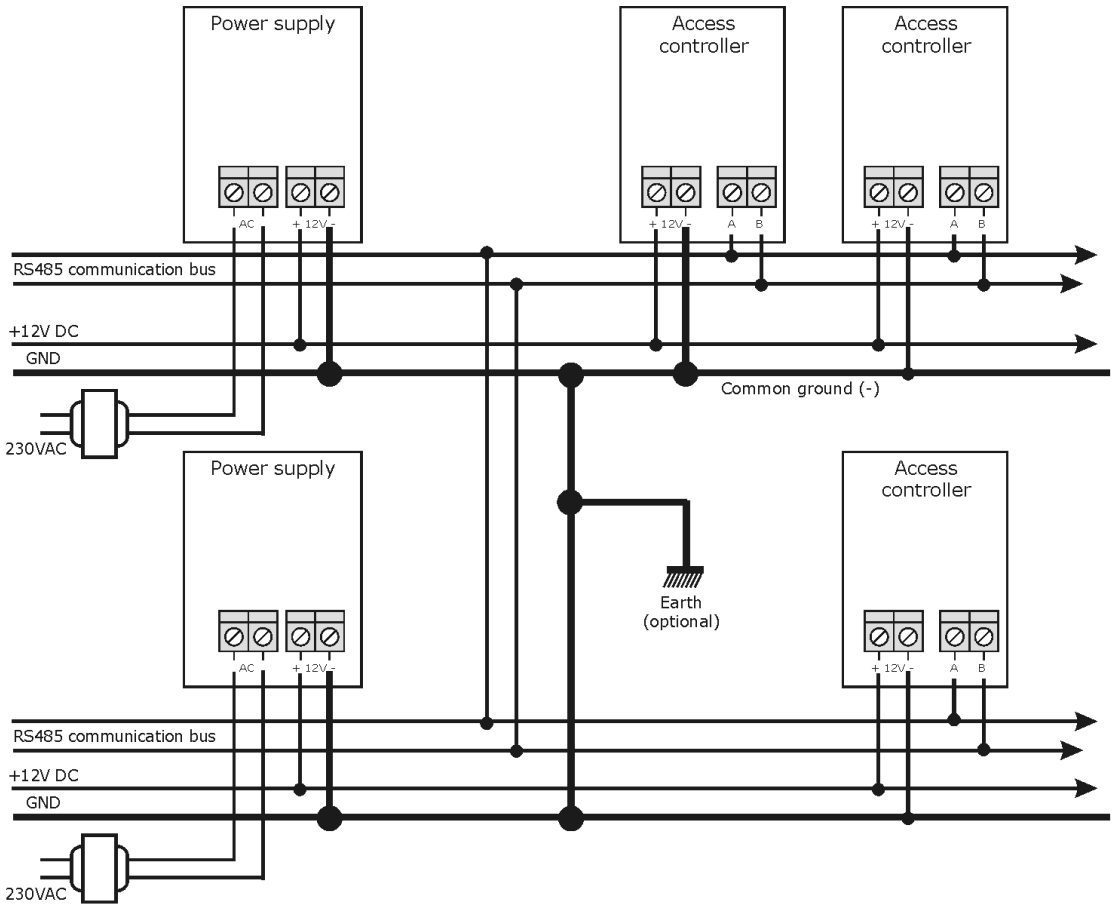
There are some settings of the device working on the EPSO 2 Protocol which can be adopted to customers requirements. These settings are kept in so called Configuration Register. The contents of the Configuration Register can be written or read using relevant communication function (see commands: “40” and “41”).

EPSO 2 Encryption Algorithm

Data send from Terminal to the Host can be encrypted using so called EPSO 2 Encryption Algorithm. The purpose of this encryption is to protect important factors like card and PIN codes from scanning by unauthorized personnel. The mechanisms of EPSO 2 Encryption Algorithm is secret and can be revealed on special request only, however customers will be asked to sign an NDA agreement.

RS485 Serial Interface

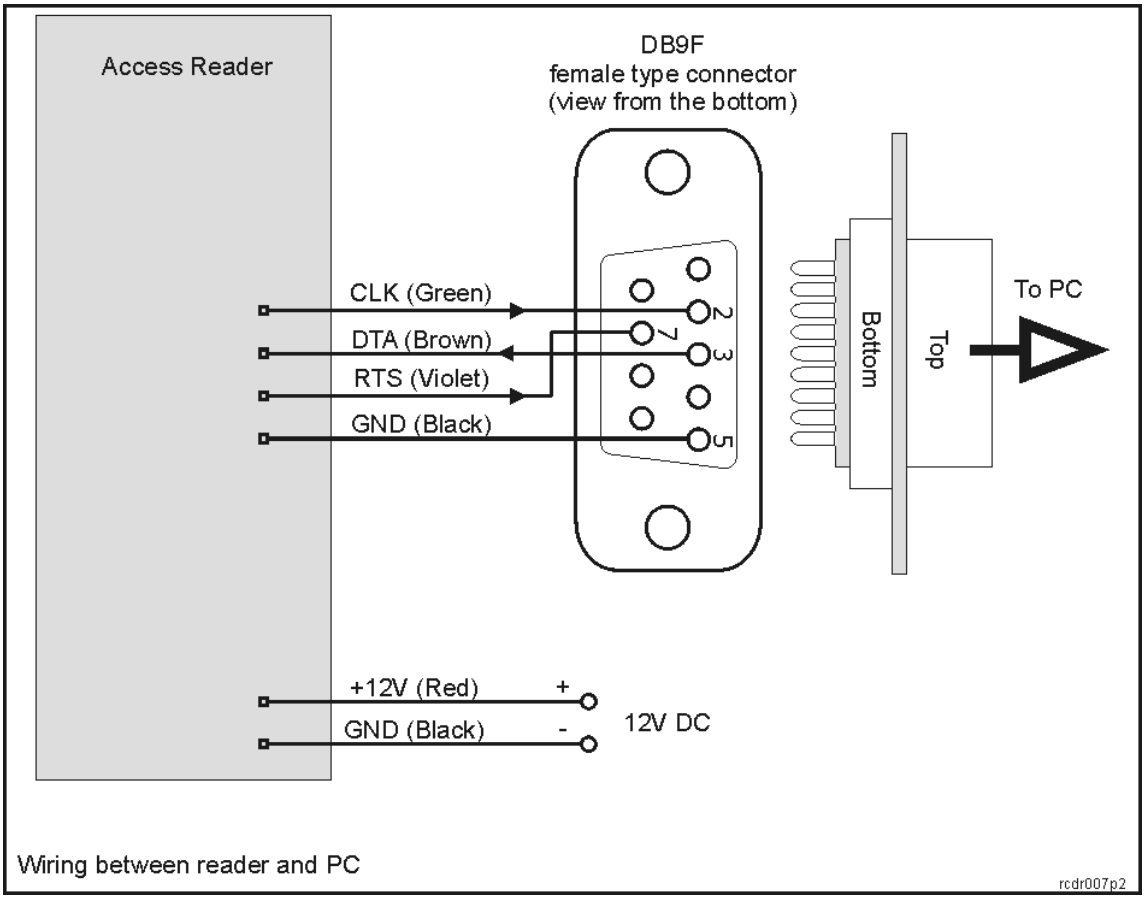
The RS485 serial interface is available on PR80 terminals only. It is possible to connect up to 32 terminals to the same communication bus however every unit must have its own individual address ranging 00-99. When using 9600 baud (or slower) transmission communication bus can be lay down using any type of signal cable however unshielded twisted pair of wires (UTP) is recommended. Also, it is possible in such a case to use free topology of communication but (any combination of three and star is allowed, no termination resistors are required on the ends of the terminal bus). The maximum distance of cable between the Host and any terminal connected to communication bus must not exceed 1200m.



Supply system and common ground (minus) arrangements (sample only) rcdr137

RS232 Serial Interface

The RS232 serial interface is available on PRT-EM and PRT-MF readers. In this case communication can be realized between Host and one Terminal only. The maximum cable run must be limited to 15m. Also, for proper communication between Host and Terminal the RTS line from the Host must be connected to the Terminal. The RTS line can be omitted in some case where TTL or CMOS levels are accepted.



Protocol Description

FRAME's FORMAT:

HEADER						DATA			CHECK
SOH	PT	ID1	ID2	FC1	FC2	STX	DATA	ETX	BCC
01	Identify	Terminal ID		Function code		02	Data	03	Checksum

- SOH, STX, ETX are the control bytes and defined as: SOH=01H, STX=02H, ETX=03H.
- PT (Packet Type) is used to identify the message, "S" means it comes from the host, and "s" means it comes from the Terminal.
- ID1 and ID2 specify address (ID number) of the Terminal, the range is from "00" to "99" (ASCI coded). Whenever required address can be changed manually by mans of **Memory Reset** or modifying **Configuration Register**.
- FC1 and FC2 are function codes, and are related to the DATA, please see the further part of description.
- BCC is the checksum, from SOH to ETX do "xor" and finally do "or" with 20H.
- The default communication baud rate is: 9600, N, 8, 1; however it can be changed through modification of the **Configuration Register**.
- Reader answers with 2ms delay and only to those frames which are addressed to it; however it can be changed through modification of the **Configuration Register**.
- There can appear the synchronization's chars (06h) between frames. They have no meanings.

FUNCTIONS

Function Code	Procedure
A1	Read card buffer
A2	Read PIN buffer
A3	Read card and PIN buffer
A5	Read card and PIN buffer and inputs (combine read command)
B0	Switch buzzer OFF
B1	Switch buzzer ON
C0	Switch Output 1 OFF
C1	Switch Output 1 ON
D0	Switch Output 2 OFF
D1	Switch Output 2 ON
D4	Switch Output 3 OFF
D5	Switch Output 3 ON
E0	Read the primary I/O status
E1	Read firmware version
E3	Set/change address (ID number)
E8	Set/clear LEDs
E9	Read the secondary I/O status
40	Write data to Configuration Register
41	Read data from Configuration Register

Notes: "DATA" means message send from the Host to the Terminal while "data" means message send from the Terminal to the Host

Function A1: Read card buffer

DATA: 1–255 (no meanings)
data: Card code

Host:

SOH	'S'	ID1	ID2	'A'	'1'	STX	DATA	ETX	BCC

Terminal:

SOH	's'	ID1	ID2	'A'	'1'	STX	data	ETX	BCC

After card is read, its code is kept in Terminal's buffer for the predefined period (2 sec. is default period). Once this period is passed by buffer is cleared and card code is erased. When Terminal has not any card read yet (buffer is empty) it sends back the STX+ETX message, but without "data". When terminal has read a card, it sends back the message with the card code on "data" position. As soon as "data" is sent back to Host the buffer is cleared and Terminal returns to reading of the cards.

The “data” consist of 17 bytes. The first byte is a letter “R’ while remaining 16 bytes are card’s code. Digits in the card number are: “0” – “9”, “A” – “F”, e.g. “00000000003EA88F”. For **Unique** type cards – first 6 digits are always 0.

Note: Optionally, this command can be encrypted using **EPSO 2 Encryption Algorithm**.

Example:
Host: SOH + ”S12A1” + STX + “42” + ETX + “&”.

Terminal: SOH + ”s12A1” + STX + ETX + 20H, means that no keypad code has been entered yet.

or

Terminal: SOH + ”s12A1” + STX + “R0000000000123456” + ETX + ‘u’ means that card was read and the card code is: “0000000000123456”.

Function A2: Read PIN buffer

DATA: 1–255 (no meanings)
data: PIN code (6 bytes max)

Host:

SOH	‘S’	ID1	ID2	‘A’	‘2’	STX	DATA	ETX	BCC

Terminal:

SOH	‘s’	ID1	ID2	‘A’	‘2’	STX	data	ETX	BCC

After PIN is entered, its code is kept in Terminal’s buffer for the predefined period (2 sec. is default period). Once this period is passed by buffer is cleared and PIN code is erased. When Terminal has not any PIN entered yet (buffer is empty) it sends back the STX+ETX message, but without “data”. When terminal has read any PIN, it sends back the message with the PIN code on “data” position. As soon as “data” is sent back to Host the buffer is cleared and Terminal returns to reading of the PINs.

The code may consist of digits: ‘0’ to ‘9’, ‘A’..’F’, the key ‘*’, and must be followed with a ‘#’ char which is interpreted as the end of a PIN code.
Coding:

Key [0] = ‘0’
Key [1] = ‘1’
..
..
..
Key [9] = ‘9’
Key [*] = ‘A’
Key [F1] = ‘C’
Key [F2] = ‘D’

If the empty PIN code is entered (only ‘#’ key is pressed), Terminal returns empty string (no chars between STX and ETX characters).

The PIN code buffer is a circular type for 6 chars, and the PIN code maximum length is 6 chars. If more keys are pressed, the next keys pressed overlap the first 6 chars.

Optionally, this command can be encrypted using **EPSO 2 Encryption Algorithm** to protect data from scanning.

Example:
Host: SOH + ”S02A2” + STX + “30” + ETX + “!”.
Terminal: SOH + ”s02A2” + STX + ETX + 22H means that no PIN code has been entered yet.
Terminal: SOH + ”s02A2” + STX + “1234” + ETX + “&” means that the PIN code “1234#” has been entered.

Function A3: Read card and PIN buffer

DATA: “1” – “255” (ignored)
data: Card code or PIN code

Host:

SOH	‘S’	ID1	ID2	‘A’	‘3’	STX	DATA	ETX	BCC

Terminal:

SOH	‘s’	ID1	ID2	‘A’	‘3’	STX	data	ETX	BCC

This function combines the “A1” and “A2” functions, so it can returns PIN or Card code. For details see description for commands A1 and A2.

Optionally, this command can be encrypted using **EPSO 2 Encryption Algorithm** to protect data from scanning.

Function A5: Read card and PIN buffer and inputs

DATA: “1” – “255” (ignored)
data: Card code and/or PIN code and/or inputs status

Host:

SOH	‘S’	ID1	ID2	‘A’	‘5’	STX	DATA	ETX	BCC

Terminal:

SOH	‘s’	ID1	ID2	‘A’	‘5’	STX	data	ETX	BCC

This function allows to read all items: card code, PIN code and inputs’ states using one complex command. The ‘data’ consists of three parts separated by the semicolon mark(:). The data are formed in following record:

CCCCCCCCCCCCC:KKKKKK:WW

Where:
CCCCCCCCCCCCC - represents card code as in the A1 function. When the Terminal has not any card read yet the card code is omitted (empty)

KKKKKK - represents PIN code as in the function A2. When the Terminal has not any PIN yet the PIN is omitted (empty)
WW - one byte, represents inputs' states; bit 0 refers to IN1, bit 1 refers to IN2, bit 2 refers to IN3, bit 3 refers to IN4, bit 4 refers to IN5, bit 5 refers to IN6 and bit 7 refers to buzzer; passive input returns 0, active input returns 1, not existing inputs return always 0. When bit 7=1 it means that buzzer is active now.

For example:

R000000AABB112233::00 AABB112233 card, no pin, all inputs OFF
:1234:01 no card, PIN 1234, input IN1 active, other inputs passive
::02 no card, no PIN, input IN2 active, other inputs and buzzer is passive.

Optionally, this command can be encrypted using **EPSO 2 Encryption Algorithm** to protect data from scanning.

Function B0: Switch Buzzer OFF

DATA: None (ignored, do not send)
data: None

Host:

SOH	'S'	ID1	ID2	'B'	'0'	STX	ETX	BCC

Terminal:

SOH	's'	ID1	ID2	'B'	'0'	STX	ETX	BCC

Example:
Host:: SOH + "S08B0" + STX + ETX + ")".
Terminal: SOH + "s08B0" + STX + ETX + "(" The buzzer is deactivated

Function B1: Switch Buzzer ON

DATA: "1" – "255"
data: "1" – "255"

Host:

SOH	'S'	ID1	ID2	'B'	'1'	STX	DATA	ETX	BCC

Terminal:

SOH	's'	ID1	ID2	'B'	'1'	STX	data	ETX	BCC

"DATA" could not be "0", otherwise it will be ignored. The range of "DATA" is "1" – "255" ("255" means the buzzer is on, till receive the function "B0"). Value of "DATA" is 0.125 sec. per one unit, for example "24" is 24 X 0.125s = 3s The message of "data" is same as "DATA"

Example:

Host: SOH + ”S07B1” + STX + “12” + ETX + “$” where DATA= “12” means the buzzer will be triggered for 1.5 sec. (12 X 0.125 = 1.5 sec.).

Terminal: SOH + ”s07B1” + STX + “12” + ETX + “$”. Buzzer is activated for 1.5s period

Function C0: Switch Output 1 OFF

DATA: None (ignored, do not send)
data: None

Host:

SOH	‘S’	ID1	ID2	‘C’	‘0’	STX	ETX	BCC

Terminal:

SOH	‘s’	ID1	ID2	‘C’	‘0’	STX	ETX	BCC

Example:
Host: SOH + ”S08C0” + STX + ETX + “(”.
Terminal: SOH + ”s08C0” + STX + ETX + “)” switches off the Output1.

Function C1”: Switch Output 1 ON

DATA: “1” – “255”
data: “1” – “255”

Host:

SOH	‘S’	ID1	ID2	‘C’	‘1’	STX	DATA	ETX	BCC

Terminal:

SOH	‘s’	ID1	ID2	‘C’	‘1’	STX	data	ETX	BCC

“DATA” would not be “0”, otherwise it will be ignored. The range of “DATA” is “1” – “255” (“255” means it would be on, till moment when Terminal receives the new command which will alter the output). Value of “DATA” is 0.125 sec., per one unit, for example “32” is 32 X 0.125 = 4 sec. The message of “data” is same as “DATA”.

Example:
Host: SOH + ”S07C1” + STX + “12” + ETX + “%” where DATA=“12” means output will be activated for 1.5 sec. (12 X 0,125s = 1.5s)

Terminal: SOH + ”s07C1” + STX + “12” + ETX + “%” means that Output 1 has been activated for 1.5s

Function D0: Switch Output 2 OFF

DATA: None (ignored, do not send)
data: None

Host:

SOH	‘S’	ID1	ID2	‘D’	‘0’	STX	ETX	BCC

Terminal:

SOH	‘s’	ID1	ID2	‘D’	‘0’	STX	ETX	BCC

Example:
Host: SOH + ”S08D0” + STX + ETX + “/” clears Output 2
Terminal: SOH + ”s08D0” + STX + ETX + “/” means that Output 2 has been cleared

Function D1: Switch Output 2 ON

DATA : “1” – “255”
data : “1” – “255”

Host:

SOH	‘S’	ID1	ID2	‘D’	‘1’	STX	DATA	ETX	BCC

Terminal:

SOH	‘s’	ID1	ID2	‘D’	‘1’	STX	data	ETX	BCC

“DATA” would not be “0” otherwise it will be ignored. The range of “DATA” is “1” – “255” (“255” triggers Output 2 for unlimited time, till moment when Terminal receives the new command which will alter the output). Value of “DATA” is 0.125 sec., per one unit, e.g. “16” is 16 X 0.125 = 2 sec. The message of “data” is same as “DATA”.

Example:
Host: SOH + ”S07D1” + STX + “12” + ETX + 22H activate Output 2 for 1.5s (12 X 0.125s =1.5s)

Terminal: SOH + ”s07D1” + STX + “12” + ETX + 22H means: that Output 2 has been activated for 1.5 seconds

Function D4: Switch Output 3 OFF

DATA: None (ignored, do not send)
data : None

Host:

SOH	‘S’	ID1	ID2	‘D’	‘4’	STX	ETX	BCC

Terminal:

SOH	‘s’	ID1	ID2	‘D’	‘4’	STX	ETX	BCC

Function D5: Switch Output 3 ON

DATA : “1” – “255”
data : “1” – “255”

Host:

SOH	‘S’	ID1	ID2	‘D’	‘1’	STX	DATA	ETX	BCC

Terminal:

SOH	‘s’	ID1	ID2	‘D’	‘1’	STX	data	ETX	BCC

"DATA" would not be "0" otherwise it will be ignored. The range of "DATA" is "1" – "255" ("255" triggers Output 2 for unlimited time, till moment when Terminal receive the new command which will alter the output). Value of "DATA" is 0.125s, per one unit, e.g. "16" is 16 X 0.125s = 2 sec. The message of "data" is same as "DATA".

Function E0: Read primary I/O status

DATA: None (ignored do not send)
data: I/O Status

Host:

SOH	'S'	ID1	ID2	'E'	'0'	STX	ETX	BCC

Terminal:

SOH	's'	ID1	ID2	'E'	'0'	STX	data	ETX	BCC

This command allows to read actual state of inputs (1 and 2), outputs (1 and 2) and buzzer. The first byte of "data" represents the status of inputs while the second byte represents a status of outputs.

Primary I/O status (two bytes)				
Input status:	**First byte**	**Input 3 (CLKIN) (Tylko PR80 od ver. 2.29.085)**	**Input 1**	**Input 2**
	0	OFF	OFF	OFF
	1	ON	OFF	OFF
	2	OFF	ON	OFF
	3	ON	ON	OFF
	4	OFF	OFF	ON
	5	ON	OFF	ON
	6	OFF	ON	ON
	7	ON	ON	ON
Output status:	**Second byte**	**Buzzer**	**Output 1**	**Output 2**
	0	OFF	OFF	OFF
	1	ON	OFF	OFF
	2	OFF	ON	OFF
	3	ON	ON	OFF
	4	OFF	OFF	ON
	5	ON	OFF	ON
	6	OFF	ON	ON
	7	ON	ON	ON

Example:
Host: SOH + "S07E0" + STX +ETX + " ! ".

Terminal: SOH + ”s07E0” + STX + “25” + ETX + “ & “ means that Input 1 is on (triggered), BUZZER and Output 2 are also ON (both set active).

Function E1: Read firmware version

DATA: None (ignored, do not send)
data: Version

Host:

SOH	‘S’	ID1	ID2	‘E’	‘1’	STX	ETX	BCC

Terminal:

SOH	‘s’	ID1	ID2	‘E’	‘1’	STX	data	ETX	BCC

Use this function order to receive the firmware version of the access Terminal.

Example:
Host: SOH + ”S07E1” + STX +ETX + “ “
Terminal: SOH + ”s07E1” + STX + “11” + ETX + “ x “ what means that the firmware version is v1.1.

Function E3: Set/change address (ID number)

DATA: ID (2 bytes)
data: ID (2 bytes)

Host:

SOH	‘S’	ID1	ID2	‘E’	‘3’	STX	DATA	ETX	BCC

Terminal:

SOH	‘s’	ID1	ID2	‘E’	‘3’	STX	data	ETX	BCC

Use this function to set the new ID (address) for Terminal. DATA is 2 byte: ‘00’ to ‘99’. The new ID is DATA: ‘00’ to ’99’ Terminal responses (answers) the message with ID1 and ID2 which are the new ID

Example:
Host: SOH + “S07E3” + STX + “02” + ETX + BCC changes address to “02”
Terminal: SOH + “s02E3” + STX + “02” + ETX + BCC answers on the new address

Function E8: Set/clear LEDs

DATA: ID (1 byte)
data: ID (1 byte)

Host:

SOH	‘S’	ID1	ID2	‘E’	‘8’	STX	DATA	ETX	BCC

Terminal:

SOH	‘s’	ID1	ID2	‘E’	‘8’	STX	data	ETX	BCC

By default all three LEDs have predefined functions as listed below:

LED ARMED (red): *Power On*
LED DISARMED (green): *No default functions*
LED OPEN (green): *Communication with the Host is OK*
LED SYSTEM (orange) *Card or PIN entered (there is some data in buffer)*

Note: The LED ARMED and DISARMED are in fact one dual color LED which can lit in read and/or green.

With the first E8 control command send from the host they become controlled externally by the host. There are following parameters available for E8 command:

DATA	**LED DISARMED Green**	**LED SYSTEM Orange**	**LED OPEN Green**	**LED ARMED Red**
'0'	OFF	OFF	OFF	OFF
'1'	OFF	ON	OFF	OFF
'2'	OFF	OFF	ON	OFF
'3'	OFF	ON	ON	OFF
'4'	OFF	OFF	OFF	ON
'5'	OFF	ON	OFF	ON
'6'	OFF	OFF	ON	ON
'7'	OFF	ON	ON	ON
'8'	ON	OFF	OFF	OFF
'9'	ON	ON	OFF	OFF
'10'	ON	OFF	ON	OFF
'11'	ON	ON	ON	OFF
'12'	ON	OFF	OFF	ON
'13'	ON	ON	OFF	ON
'14'	ON	OFF	ON	ON
'15'	ON	ON	ON	ON
16 – 255	*The values between 16-255 switch LEDs to default functions*			

Function 40: Write Configuration Register

DATA: ZLRTTCCPP
data: Status

Host:

SOH	'S'	ID1	ID2	'4'	'0'	STX	DATA	ETX	BCC

Terminal:

SOH	‘s’	ID1	ID2	‘4’	‘0’	STX	data	ETX	BCC

This function allows to write data do **Configuration Register**.

DATA sector consist of following record: **ZLRTTCCPP**

Where:

Z=’0’..’5’
Z sets *Buzzer loudness level*: ‘0’-0%,‘1’-20%,‘2’-40%,‘3’-60%,‘4’-80%,‘5’-100%

L=’0’..’5’
L sets *Keypad backlight level*: ‘0’-0%,‘1’-20%,‘2’-40%,‘3’-60%,‘4’-80%,‘5’-100%

R=’1’..’6’
R sets *Communication baud rate*: ‘1’-1200B, ‘2’-2400B, ‘3’-4800B, ‘4’-9600B, ‘5’-19200B,‘6’-38400B

TT=‘00’..’FF’ (BCD: one byte coded as two hexadecimal chars)
TT sets *Communication lost timeout* in ½ seconds, setting value above 240 (120 sec.) deactivates this timeout. When Terminal will not receive any command from Host for time declared by this timeout it will start pulsing all LED-s however with next command received from Host it will return to normal LED indication.

CC=‘00’..’FF’ (BCD: one byte coded as two hexadecimal chars)
CC sets *Card/PIN buffer timeout* in ½ seconds, setting value above 240 (120 sec.) deactivates this timeout. When the card/PIN buffer will not be read within time specified by this parameter reader will automatically clear card/PIN buffer.

PP=‘00’..’FF’ (BCD: one byte coded as two hexadecimal chars)
PP represents three *Advanced options*:
All options are set 1 as default (PP=‘FF’).

When **bit 0=0** then LED_SYSTEM indicates valid card/ PIN code in the buffer
When **bit 0=1** then LED_SYSTEM work in normal mode (controlled by the host)

When **bit 1=0** then reader doesn’t allow to read a new card or Pin till moment when buffer is read by the host or cleared by the timeout (see: Card/Pin buffer timeout)
When **bit 1=1** then reader allow to read a new card or Pin even when buffer is not empty.

When **bit 2=0** then card/PIN data in communication frames is encrypted using EPSO 2 Encryption Algorithm (EEA)
When **bit 2=1** then card/PIN data in communication frames is not encrypted in any way

Note: In order to leave some parameter(s) in Configuration Register unchanged use “– “ character.

For example:
Writing **34548– –FF** sets following options:
- *Buzzer loudness level* 60% (because Z='3')
- *Keypad backlight level* 80% (because L='4')
- *Communication baud rate* 19200 (because R='5')
- *Communication lost timeout* 24s (because TT='48')
- *Card/PIN buffer timeout* remains unchanged (because CC='– –')
- All *Advanced options* switched OFF (because PP='FF')

Function 41: Read Configuration Register

DATA: None
data: ZLRTTCCPP

Host:

SOH	'S'	ID1	ID2	'4'	'1'	STX	DATA	ETX	BCC

Terminal:

SOH	's'	ID1	ID2	'4'	'1'	STX	data	ETX	BCC

This function allows to read contents of the **Configuration Register**. The "data" sector consist of identical record (**ZLRTTCCPP**) as in the function 40.

Memory Reset

The **Memory Reset** procedure resets current Terminal's settings, restores factory defaults and configures device to work in EPSO 2 Protocol mode.

Memory Reset procedure:

- Power down the unit
- Connect CLK to IN1 lines
- Restore power, Terminal will generate a continues sound, LED ENTER will blink
- Remove connection between CLK and IN1 lines. Terminal will blink LED STATUS.
- Define work mode of the terminal as 040 (3 digits).
  (skip this step when using EPRT firmware).
- Terminal restarts.

After the last step Terminal switches Configuration Register to defaults and sets reader address ID=00.

Defaults:
- *Buzzer loudness level* 60% (Z=3)
- *Keypad backlight level* 60% (L=3)
- *Communication baud rate* 9600B (R=4)
- *Communication lost timeout* 20s (TT=28)
- *Card/PIN buffer timeout* 2s (CC=04)
- *Advanced option* switched OFF (because PP=FFH)

Roger sp. j.

82-400 Sztum

Gościszewo 59

Tel.: +48 55 272 01 32

Fax: +48 55 272 01 33

Technical support PSTN: +48 55 267 01 26

e-mail: biuro@roger.pl