Application Note 428

Title: **EM4095 RFID Reader Firmware Protocol Description**

Product Family: **RFID**

Part Number: EMDB409

Keywords: EM4095, EMDB409, ISO 11784/ 11785, Animal, Read Only, EM4200, EM4450, EM4205, EM4305, EM6869

Date: March 4, 2010

1. Introduction

EMDB409 reader is a base station for communication with a selected set of 125 kHz transponders. This AN428 application note describes an EMDB409 firmware communication protocol.

Version	Source name tree	Last Release	Description
90	EMDB409_firmware_standard	0.15 (9.10.2009)	EM4095 RFID READER Firmware

Table 1: Existing firmware families

Transponder family	Command set support	Coding and data rate support
EM4200	Animal mode – Single Read Read Only mode – Single Read	Bi/32 Mn/32, Mn/64, Bi/32, Bi/64
EM4450	All	Mn/64, Mn/32
EM4205/EM4305	All	Mn/32, Mn/64, Bi/32, Bi/64
EM6869	All except Select Page, Read Word 0-31, and Write Word 0-31	Mn/32

Table 2: Family 90 supported command set and features

Note: Mn/32 means Manchester encoding with Data Rate RF/32, Bi means bi-phase, etc.

2. Description of the communication protocol

The firmware main loop periodically analyze the UART receive buffer and performs particular actions on valid messages. All performed actions or detected errors emit a response message. The UART data reception is performed asynchronously. No next message analysis is generated until the response on previous action is sent out.

2.1. Communication parameters

The commands and their responses are transmitted on USB line. The microcontroller does not integrate a USB port directly. Therefore, USB to serial line converter is used to translate the USB packets to the serial line of the microcontroller.

The communication parameters are unified. For more information, please, refer to the firmware sources Readme.txt (description serial line communication parameters).

2.2. Message format

All messages follow the next rules:

- Byte[0] = STX = 02h
- Byte[1] = index of checksum byte = last-1
- Byte[2] = command/response identification
- Byte[3..last-2] = payload
- Byte[last-1] = XOR checksum = Byte[1] XOR Byte[2] XOR .... XOR Byte[last-2]
- Byte[last] = ETX = 03h

2.3. PC to reader (Command)

Each command sent by the EM4095 Reader to the transponder is initiated by a supplied command from PC software application, e.g.; EMDB409 Reader Application Software. The PC command set comprises the following groups:

- Animal mode and Read Only mode commands (EM4200)
- EM4450 commands
- EM4205/EM4305 commands
- EM6869 commands
- Reader Control commands

Commands supported by current firmware are shown in following tables.

PC to reader	Serial Data Bytes sent on UART											
Command	0	1	2	3	4	…					xx-1	xx
Animal mode commands (EM4200, EM4205/EM4305)												
Single Read	02h	03h	11h	12h	03h							
Read Only mode commands (EM4200, EM4205/EM4305)												
Autodetect Single Read	02h	03h	10h	13h	03h							
EM4450 commands												
Login	02h	08h	30h	01h	MSB <4 Bytes> LSB current password			CHK	03h			
New Password	02h	0Ch	31h	01h	MSB <4 Bytes> LSB current password			MSB <4 Bytes> LSB new password			CHK	03h
Write Block	02h	08h	32h	Addr	MSB <4 Bytes> LSB new value			CHK	03h			
Set Control Word	02h	08h	32h	02h	MSB <4 Bytes> LSB new value of control word			CHK	03h			
Read Block	02h	08h	33h	00h	00h	00h	Addr	Addr	CHK	03h		
Selective Read	02h	08h	33h	00h	00h	00h	LBR	FBR	CHK	03h		
Reset	02h	03h	34h	37h	03h							
Read In Control Word	02h	03h	35h	36h	03h							
EM4205/EM4305 commands												
Read Block	02h	04h	90h	Addr	CHK	03h						
Write Block	02h	08h	91h	Adrr	LSB <4 Bytes> MSB new value			CHK	03h			
New Password	02h	08h	91h	02h	LSB <4 Bytes> MSB new password value			CHK	03h			
Configuration	02h	08h	91h	04h	LSB <4 Bytes> MSB configuration value			CHK	03h			
Login	02h	07h	92h	LSB <4 Bytes> MSB current password value			CHK	03h				
Disable	02h	03h	93h	80h	03h							
Protect	02h	08h	97h	LSB <4 Bytes> MSB protection value			CHK	03h				

PC to reader	Serial Data Bytes sent on UART											
EM6869 commands												
LF Wake-up	02h	03h	A0h	A3h	03h							
Read Word 0-1023	02h	05h	A1h	LSB <2 Bytes> MSB addr			CHK	03h				
Write Word 0-1023	02h	07h	A2h	LSB <2 Bytes> MSB addr			LSB <2 Bytes> MSB data word			CHK	03h	
Read Page	02h	xx-1	A3h	LSB <2 Bytes> MSB addr		LWR	CHK	03h				
Write Page	02h	xx-1	A4h	LSB <2 Bytes> MSB addr		LWR	<2N Bytes> {LSB,MSB} data words		CHK	03h		
Authenticate/UnlockUM	02h	xx-1	A5h	Auth mode	MSB <0-16 Bytes> LSB RN			MSB <4-16 Bytes> LSB F			CHK	03h
Unlock Key	02h	0Bh	A6h	MSB <4 Bytes> LSB ID[31:0]			MSB <4 Bytes> LSB SK1[31:0]			CHK	03h	
GetRN1	02h	04h	A7h	Len	CHK	03h						
Send Access	02h	0Bh	A8h	MSB <4 Bytes> LSB ID[31:0]			MSB <4 Bytes> LSB Password[31:0]			CHK	03h	
Reader Control commands												
Field Reset	02h	04h	F0h	FFh	0Bh	03h						
Switch to bootloader	02h	03h	F3h	F0h	03h							
Reader Get Configuration	02h	03h	FBh	FFh	03h							
Reader Set New Configuration	02h	07h	FCh	LSB <4 Bytes> MSB configuration value			CHK	03h				
Reader Version	02h	03h	FDh	FEh	03h							
Field ON	02h	04h	FEh	01h	FBh	03h						
Field OFF	02h	04h	FEh	00h	FAh	03h						

Note:

- All values are in a hexadecimal format
- LSB, MSB - low endian bytes ordering
- LBR, FBR - Last/First Block Read

- SM - Scan Mode = 00h – Free running mode, 01h - Switch off/Slow down mode, FFh – stop scan

2.4. Reader to PC (Response)

Reader to PC	Serial Data Bytes sent on UART											
Response	0	1	2	3	4	…					xx-1	xx
Animal mode commands												
Single Read ACK = 00h	02h	14h	11h	00h	UC D13- D00	LSB <4 bytes> MSB Unique Serial Number				Last data byte	CHK	03
Single Read ACK ≠ 00h	02h	04h	11h	ACK	CHK	03h						
EM4100 commands												
Autodetect **Single Read** ACK = 00h	02h	09h	10h	00h	First data byte	…				Last data byte	CHK	03
Autodetect **Single Read** ACK ≠ 00h	02h	04h	10h	ACK	CHK	03h						
EM4x50 commands												
Login	02h	04h	30h	ACK	CHK	03h						
New Password	02h	04h	31h	ACK	CHK	03h						
Write Block	02h	04h	32h	ACK	CHK	03h						
Set Control Word	02h	04h	32h	ACK	CHK	03h						
Read Block ACK = 00h	02h	09h	33h	00h	Addr	LSB <4 Bytes> MSB value on address Addr			CHK	03h		
Read Block ACK ≠ 00h	02h	04h	33h	ACK	CHK	03h						
Selective Read ACK = 00h	02h	09h	33h	00h	FBR	LSB <4 Bytes> MSB value in Block FBR			CHK	03h		
	02h	09h	33h	00h	FBR +1	LSB <4 Bytes> MSB value on Block FBR+1			CHK	03h		

Reader to PC	Serial Data Bytes sent on UART											
	..	..	..	..	..	…	..	..				
	02h	09h	33h	00h	LBR	LSB <4 Bytes> MSB value on Block LBR			CHK	03h		
Selective Read ACK ≠ 00h	02h	04h	33h	ACK	CHK	03h						
Reset	02h	04h	34h	ACK	CHK							
Read In Ctrl. Word ACK = 00h	02h	09h	35h	00h	FBR	LSB <4 Bytes> MSB value in Block FBR			CHK	03h		
	02h	09h	35h	00h	FBR +1	LSB <4 Bytes> MSB value on Block FBR+1			CHK	03h		
	..	..	..	..	..	…	..	..				
	02h	09h	35h	00h	LBR	LSB <4 Bytes> MSB value on Block LBR			CHK	03h		
Read In Ctrl. Word ACK ≠ 00h	02h	04h	35h	ACK	CHK	03h						
EM4205/EM4305 commands												
Read Block ACK = 00h	02h	09h	90h	00h	Addr	LSB <4 Bytes> MSB value on address Addr.			CHK	03h		
Read Block ACK ≠ 00h	02h	09h	90h	ACK	Addr	<4 Bytes> 00h 00h 00h 00h			CHK	03h		
Write Block	02h	04h	91h	ACK	CHK	03h						
New Password	02h	04h	91h	ACK	CHK	03h						
Configuration	02h	04h	91h	ACK	CHK	03h						
Login	02h	04h	92h	ACK	CHK	03h						
Disable	02h	04h	93h	ACK	CHK	03h						
Protection	02h	04h	97h	ACK	CHK	03h						
EM4869 commands												
LF Wake-up	02h	04h	A0h	ACK	CHK	03h						

Reader to PC	Serial Data Bytes sent on UART											
Read Word 0-1023 ACK == 0	02h	06h	A1h	00h	LSB MSB word		CHK	03h				
Read Word 0-1023 ACK <> 0	02h	04h	A1h	ACK	CHK	03h						
Write Word 0-1023	02h	04h	A2h	ACK	CHK	03h						
Read Page	02h	xx-1	A3h	ACK	LSB <4 bytes> MSB status			LSB <N words> MSB words			CHK	03h
Write Page	02h	08h	A4h	ACK	LSB <4 bytes> MSB status			CHK	03h			
Authenticate/Unlock UM	02h	xx-1	A5h	ACK	MSB <4-16 Bytes> LSB G			CHK	03h			
Unlock Key	02h	04h	A6h	ACK	CHK	03h						
GetRN1	02h	xx-1	A7h	ACK	MSB <4-16 Bytes> LSB RN			CHK	03h			
Send Access	02h	04h	A8h	ACK	CHK	03h						
Reader Control commands												
Field Reset	02h	04h	F0h	ACK	CHK	03h						
Bootloader Mode	02h	04h	F3h	ACK	CHK	03h						
Reader Get Configuration	02h	07h	FBh	LSB <4 Bytes> MSB configuration value			CHK	03h				
Reader Set New Configuration	02h	04h	FCh	ACK	CHK	03h						
Reader Version	02h	08h	FDh	ACK	Release	Date	Version	CHK	03h			
Field ON	02h	04h	FEh	ACK	CHK	03h						
Field OFF	02h	04h	FEh	ACK	CHK	03h						

Note:

- All values are in a hexadecimal format
- LSB, MSB - low endian bytes ordering
- LBR, FBR - Last/First Block Read
- UC – Read Only data structure Customer Code, MSBit corresponds to D13 bit, LSBit corresponds to D00 bit
- Unique Serial Number – Read Only data structure serial number, MSBit of LSByte corresponds to D93 bit, LSBit of MSByte is D20 bit.

2.5. ACK byte

ACK set to 00h always signalises successful execution of the command, otherwise non-zero ACK values signalise errors or other information.

UART errors are common to all the commands, they signalise a problem during PC<->Reader communication or protocol errors.

Antenna fault (01h) error is common to all the commands. Antenna fault error is generated automatically on microcontroller watchdog time-out after 2 sec signalising the operation could not be terminated standard way.

Generally, the commands that communicate with the tags successfully (i.e., ACK = 00h) return a data bytes already decoded.

ACK value	Symbolic Name	Fault from part
00h	UART_MESSAGE_OK	All parts (command completed successfully)
01h	ERR_ASIC_ANTENNA_FAULT	ASIC + Reader
04h	ERR_UART_ERROR_FLAG	UART (none ot wrong STX, parity error)
05h	ERR_UART_OVERFLOW	UART (command too long to be received by the reader)
06h	ERR_UART_WRONG_ICMD	UART (incorrect command parameters)
07h	ERR_UART_BAD_CRC	UART
08h	ERR_UART_UNKNOWN_CMD	UART (command code is not supported by this firmware)
09h	ERR_UART_NO_ETX	UART (ETX not found after the position specified in 2nd byte)
0Ah	ERR_UART_INTERBYTE_ERR	UART (message length is out of range, message length is wrong with this command)
0Bh	ERR_EM4469_FLOWLINK_ERR	Reader (bad RDY/CLK signal or bad/noisy DEMOD_OUT signal, not enough data, wrong decoding parameters)
0Ch	ERR_EM4469_WRONG_DE	Reader (wrong encoding in Configuration word)
0Dh	ERR_EM4469_WRONG_DR	Reader (wrong data rate in Configuration word)
10h	ERR_EM4469_PARITY_ERR	Reader (bad parity in read word response, noisy data)
11h	ERR_EM4469_BAD_CONF_DATA	Reader (wrong lwr in Configuration word, wrong FwLink value)
12h	ERR_EM4469_NACK	Reader (no acknowledge detected)
13h	ERR_EM4469_NEITHER_ACK	Reader (neither ack or nack detected)
14h	ERR_EM4469_NO_VALID_DR	Reader (no valid default read detected)
15h	ERR_EM4469_BAD_RAW	Reader (unequal read after write data)
21h	ERR_TIMEOUT_TXP	Reader (time for response from transponder is out)
22h	ERR_HEADER_READ_FAULT	Reader (header not found)
23h	ERR_READ_ID_FAULT	Reader (UID not found)
24h	ERR_READ_ID_CHK_FAULT	Reader (checksum error in read response)

ACK value	Description	Fault from part
26h	ERR_NO_LIW	Reader (not found Listen Window)
27h	ERR_WRONG_ADDRESS	Reader (wrong address for reading)
28h	ERR_WRONG_DATA	Reader (invalid bit in read response)
29h	ERR_PARITY_ERROR	Reader (bad parity in read word response, noisy data)
2Ah	ERR_NACK_RECEIVE	Reader (no Acknowledge detected)
2Bh	UART_MESSAGE_NACK	Reader (Nack-ed correct behaviour)
34h	ERR_EM4026_NOUID	Reader (UID not found, EM4026)
35h	ERR_EM4026_RAW_DATA	Reader (unequal read after write data)
41h	ERR_EM6869_TIMEOUT_TXP	Reader (unexpected pattern observed)
42h	ERR_EM6869_NO_IP	Reader (no IP pattern observed, reader cannot start the transmission)
43h	ERR_EM6869_NACK_RECEIVED	Reader (NACK pattern received)
44h	ERR_EM6869_PARITY_ERROR	Reader ()
45h	ERR_EM6869_PREAMBLE_ERROR	Reader (LF preamble contents mismatch)
46h	ERR_EM6869_WRONG_DATA	Reader ()
47h	ERR_EM6869_BAD_DATA	Reader ()
48h	ERR_EM6869_TIMEOUT_RXP	Reader (neither ACK or NACK received)

2.6. Antenna fault (01h) error

Antenna fault (01h) error is common to all the commands. Antenna fault error is generated automatically on microcontroller watchdog time-out after 2.1s signalising the operation could not be terminated standard way.

The known operation that could not be terminated standard way is a data capture process of communication commands that uses an interrupt. Because of limited interrupt priority scheduling and with a certain type of input data signals, the data capture process stop condition has less priority to be executed. Therefore, watchdog is used to interrupt the data capture process, and Antenna Fault (01h) error has to be treated as standard result.

2.7. Command Description

Following subchapters describe each command behaviour and its possible errors. UART communication errors are common to all the commands and are omitted here. Antenna fault (01h) error is also common to all the commands.

2.7.1. Read Only mode – Autodetect Single Read (10h)

Single Read command for Read Only mode compliant transponders (EM4200, EM4205/EM4305) reads 64 bit Identification number (UID) of single transponder in the RF field. Reader tries the following encodings/data rate settings; Mn/64, Mn/32, Bi/64, Bi/32.

Possible error codes: 23h, 24h

2.7.2. Animal mode - Single Read (11h)

Single Read command for Animal mode compliant transponders (EM4200, EM4205/EM4305) reads 128 bit Animal mode data structure of single transponder in the RF field.

Possible error codes: 23h

2.7.3. Login (30h) - EM4450

After reception of this command the reader is finding the Listen Window (LIW). If the reader finds out LIW in demodulated stream from the transponder, the reader subsequently sends RM pattern, command data bits for Login function and bits of the password value. Then the reader waits for processing pause time (tpp). Upon tpp the reader receives answer from the transponder and sends answer to the Application software.

Possible error codes: 21h, 26h, 2Ah

2.7.4. New Password (31h) - EM4450

After reception of this command the reader is finding the Listen Window (LIW). If the reader finds out LIW in demodulated stream from the transponder, the reader subsequently sends RM pattern, command data bits for Write Password function and bits of the actual password value. Then the reader waits for processing pause time (tpp). Upon tpp the reader receives answer from the transponder. If the answer is ACK then the reader finds LIW and sends RM pattern with bits of the new password value. Then the reader receives answer from the transponder and sends answer to the Application software.

Possible error codes: 21h, 26h, 2Ah

2.7.5. Write Block (32h) - EM4450

After reception of this command the reader is finding the Listen Window (LIW). If the reader finds out LIW in demodulated stream from the transponder, the reader subsequently sends RM pattern with command data bits for Write Word function, bits of the block address and bits of the new value. Then the reader waits for write access time (twa). Upon twa the reader receives answer from the transponder and sends answer to the Application software.
Possible error codes: 21h, 26h, 2Ah

2.7.6. Set Control Word (32h) - EM4450

Set Control Word command has the same running as Write Block (32h) command. Difference is only in the word address value. The word address value is 02h for this command.

Possible error codes: 21h, 26h, 2Ah

2.7.7. Selective Read (33h) - EM4450

After reception of this command the reader is finding the Listen Window (LIW). If the reader finds out LIW in demodulated stream from the transponder, the reader subsequently sends RM pattern with command data bits for Selective Read Mode function and bits for the Last Block Read (LBR) address and First Block Read (FBR) address. Then the reader waits for processing pause time (tpp). Upon tpp the reader receives answer from the transponder and sends answer to the Application software.

Possible error codes: 21h, 26h, 27h, 28h, 29h, 2Ah

2.7.8. Read Block (33h) - EM4450

Read Block command has the same running as Selective Read (33h) command. Difference is only that the value of Last Block Read = First Block Read = Address of the read block.

Possible error codes: 21h, 26h, 27h, 28h, 29h, 2Ah

2.7.9. Reset (34h) - EM4450

After reception of this command the reader is finding the Listen Window (LIW). If the reader finds out LIW in demodulated stream from the transponder, the reader subsequently sends RM pattern with command data bits for Reset function. Then the reader waits for processing pause time (tpp). Upon tpp the reader receives answer from the transponder and sends answer to the Application software.

Possible error codes: 21h, 26h, 2Ah

2.7.10. Read In Control Word (35h) - EM4450

After reception of this command the reader executes the sequence for the Read Block command with Address for the reading block = 2. If the reader receives value from block 2 then the reader executes sequence for the Selective Read Command with values for LBR and FBR from the block 2.

Possible error codes: 21h, 26h, 27h, 28h, 29h, 2Ah

2.7.11. Read Block (90h) - EM4205/EM4305

After reception of this command the reader sends command data bits of Read Word command and address bits of the reading word. Then the reader waits for processing pause time (tpp). Upon tpp the reader receives answer from the transponder and sends answer to the Application software.

Possible error codes: 0Bh, 10h, 12h, 13h.

2.7.12. Write Block (91h) - EM4205/EM4305

After reception of this command the reader sends command data bits of Write Word command, address bits of the write word and new value of the write word. Then the reader waits for EEPROM programming time (t_{Wee}). Upon t_{Wee} the reader receives answer from the transponder and sends answer to the Application software. Actually, the reception is already enabled after tpp time so that a NACK can be captured.

Possible error codes: 0Bh, 10h, 12h, 13h, 15h.

2.7.13. Login (92h) - EM4205/EM4305

After reception of this command the reader sends command data bits of Login command and actual password value. Then the reader waits for processing pause time (tpp). Upon tpp the reader receives answer from the transponder and sends answer to the Application software.

Possible error codes: 0Bh, 10h, 12h, 13h.

2.7.14. Disable (93h) - EM4205/EM4305

After reception of this command the reader sends command data bits of Disable command. The EM4205 or EM4305 accepts disable command only when the Disable bit in Tag Special Bits is set to 1. When the Disable command is accepted, the EM4205 or EM4305 stops all operations until next power-up. In case the Disable command is not accepted, EM4205 or EM4305 tag returns in Default Read mode.

Possible error codes: 0Bh, 12h, 13h

2.7.15. Protect (97h) - EM4205/EM4305

After reception of this command the reader sends command data bits of the Protect command and a value of the protection word (EM4205/EM4305 tag performs the logical OR of the current protection word and the word provided by the Protect command). Then the reader waits for Protection word update time (t_{pr}). Upon t_{pr} the reader receives answer from the transponder and sends answer to the Application software. Actually, the reception is already enabled after tpp time so that a NACK can be captured.

Possible error codes: 0Bh, 10h, 12h, 13h, 15h.

2.7.16. LF Wakeup (A0h) – EM6869

The reader synchronizes itself to incoming IP pattern and transmits the LF Wakeup command. Then it waits for Tpp time and receives the ACK and LF preamble.

Possible error codes: 42h, 41h, 45h, 48h.

2.7.17. Read Word (A1h) – EM6869

The reader synchronizes itself to incoming IP pattern and transmits the Read Word (0-1023) command with the address addr. Then it waits for Tpp time and receives the ACK. + LF preamble + 1 word data block or NACK pattern.

Possible error codes: 42h, 41h, 45h, 48h, 43h, 44h.

2.7.18. Write Word (A2h) – EM6869

The reader synchronizes itself to incoming IP pattern and transmits the Write Word (0-1023) command with address addr and data word supplied as the parameters. Then it waits for Tpp time and receives the ACK. + LF preamble or NACK pattern.

Possible error codes: 42h, 41h, 45h, 48h, 43h.

2.7.19. Read Page (A3h) – EM6869

The reader uses Read Word (0-1023) command multiple times to read the sequence of words specified at starting address addr and ending at address LWR of the same page, i.e. the last read word address is (addr AND NOT(31)) OR LWR, 32 words at maximum. LWR item may be lower than addr (mod 32). If LWR equals addr (mod 32) the whole page is read.

The status response item is 32b mask for each word within the addressed page, the bit at the corresponding word address position is set to 1 if either read data is valid (word is within the range) or the word has not been read (word is outside the range). The bit at the corresponding word address position is set to 0 if either the read operation returned NACK or the read operation failed. Whenever the read operation fails with no ACK/NACK recognized, the read operation is tried 2 times more.

Note: The reader total processing timeout is limited to 2.2s. With always successful operation, the whole page read takes about 50ms x 32 = 1.6sec. In case the one or more read operations is repeated because of noisy environment or malfunctioning tag, the total time can exceed 2.2sec reader timeout and Antenna fault response is returned. Antenna fault response signalises the communication with the tag is not sufficient the application software shall reset or switch on the RF field in order to continue with communication.

Possible error codes: 42h, 41h, 45h, 48h, 43h.

Example:

```
EM6869 : Read Page
Sent: |02 06 A3 00 00 1F BA 03|
Received: <02 48 A3 00 FF FC 03 00 69 68 00 00 FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 EA 03 >
OK
Value in Block 0 (0x000) is : 0x6869
Value in Block 1 (0x001) is : 0x0000
Value in Block 2 (0x002) is : 0xFFFF
Value in Block 3 (0x003) is : 0x0000
Value in Block 4 (0x004) is : 0x0000
Value in Block 5 (0x005) is : 0x0000
Value in Block 6 (0x006) is : 0x0000
Value in Block 7 (0x007) is : 0x0000
Value in Block 8 (0x008) is : NACK
Value in Block 9 (0x009) is : NACK
Value in Block 10 (0x00A) is : 0x0000
Value in Block 11 (0x00B) is : 0x0000
Value in Block 12 (0x00C) is : 0x0000
Value in Block 13 (0x00D) is : 0x0000
Value in Block 14 (0x00E) is : 0x0000
Value in Block 15 (0x00F) is : 0x0000
Value in Block 16 (0x010) is : 0x0000
Value in Block 17 (0x011) is : 0x0000
Value in Block 18 (0x012) is : NACK
Value in Block 19 (0x013) is : NACK
Value in Block 20 (0x014) is : NACK
Value in Block 21 (0x015) is : NACK
Value in Block 22 (0x016) is : NACK
Value in Block 23 (0x017) is : NACK
Value in Block 24 (0x018) is : NACK
Value in Block 25 (0x019) is : NACK
Value in Block 26 (0x01A) is : NACK
Value in Block 27 (0x01B) is : NACK
Value in Block 28 (0x01C) is : NACK
Value in Block 29 (0x01D) is : NACK
Value in Block 30 (0x01E) is : NACK
Value in Block 31 (0x01F) is : NACK
```

2.7.20. Write Page (A4h) – EM6869

Write Page Range command writes 1 to 16 words into the words in range from addr to LWR within the same page using Write Word (0-1023) command. Maximum number of words is 16. LWR is always equal or higher than addr (mod 32).

The status response item is 32b mask for word within the addressed page, the bit at the corresponding word address position is set to 1 if either written data was successful (word is within the range) or the word has not been written (word is outside the range). The bit at the corresponding word address position is set to 0 if either the read operation returned NACK or the read operation failed.

Whenever the read operation fails with no ACK/NACK recognized, the read operation is tried 2 times more.

The same timeout applies for this command as same as for Read Page Range command.

Possible error codes: 42h, 41h, 45h, 48h, 43h.

Example:

```
EM6869 : Write Page
 Sent: |02 0C A4 43 00 05 34 12 78 56 BC 9A C0 03|
 Received: <02 08 A4 00 FF FF FF FF AC 03 >
 OK
 nack = FFFFFFFF
 Value in Block 67 (0x043) is : 0x1234
 Value in Block 68 (0x044) is : 0x5678
 Value in Block 69 (0x045) is : 0x9ABC
```

2.7.21. Authenticate/UnlockUM (A5h) – EM6869

Authentication command performs an authentication command according to the Auth mode parameter.

Auth mode byte binary structure is 'AAGGFFRR'b, where GG is the length of the G function number, FF is the length of F function number, and RR is the length of RN number, all lengths are a number of 32b words units minus 1.

- When AA is '00' the Mutual Authentication is performed
- When AA is ‘01’ the Mutual Authentication is performed
- When AA is '10' the Mutual ISO Authentication is performed
- When AA is ‘11’ the Unlock UM command is performed

Mutual ISO Authentication drops the RN item from the Command structure.

The reader application software is responsible for using matching GG, FF, and RR length as configured in the tag.

Possible error codes: 42h, 41h, 45h, 48h, 43h.

2.7.22. Unlock Key (A6h) – EM6869

Unlock Key command performs Unlock Key command with ID and part of SK1 key.

Possible error codes: 42h, 41h, 45h, 48h, 43h.

2.7.23. Get RN (A7h) – EM6869

Reader transmits GetRN command and captures the response. Firmware assumes the returned response contains the number of 32b random words that equals (Len (mod 4) + 1). The reader application software is responsible for using matching RR as configured in the tag.

Possible error codes: 42h, 41h, 45h, 48h, 43h.

2.7.24. Send Access (A8h) – EM6869

Reader transmits the Send Access command with ID and Password.

Possible error codes: 42h, 41h, 45h, 48h, 43h.

2.7.25. Field Reset (F0h) - Reader

Field Reset command switches off and switches on the RF field for a specified time interval.

2.7.26. Switch to bootloader (F3h) - Reader

After receiving the command Switch to bootloader, the microcontroller switches the RF field and enters the bootloader mode so that the new firmware can be updated. See Bootloader chapter for further details.

2.7.27. Reader Get Configuration (FBh) – Reader

The current configuration word stored in the microcontroller can be read back to the PC by means of the Reader Get Configuration command. The configuration word format is the same as described in Reader Set New Configuration (FCh) command.

2.7.28. Reader Set New Configuration (FCh) – Reader

The configuration contains the settings which the reader should use for communication with tags. The values are the same as defined in EM4469 datasheet.

Configuration item	Range in configuration word	Description
Data Rate	[5:0]	Current reader data rate
Encoder	[9:6]	Current decoding type
reserved	[13:10]	All bits are set to 0
LWR	[17:14]	Current number of read word in default read
reserved	[31-18]	All bits are set to 0

2.7.29. Reader Status (FDh) - Reader

Reader Status command response contains Version (family), Release and Release date of the firmware. Release is defined as a number in "BCD" format (e.g.: 0Ch => release 0.12). Date of the release is coded in format: year[15:10], month[9:6], day[5:0]. Year value = 0 is the year 2K.

2.7.30. Field ON/OFF (FEh) - Reader

Field ON sets the SHD pin = 0 according to the EM4095 data sheet.

3. Bootloader

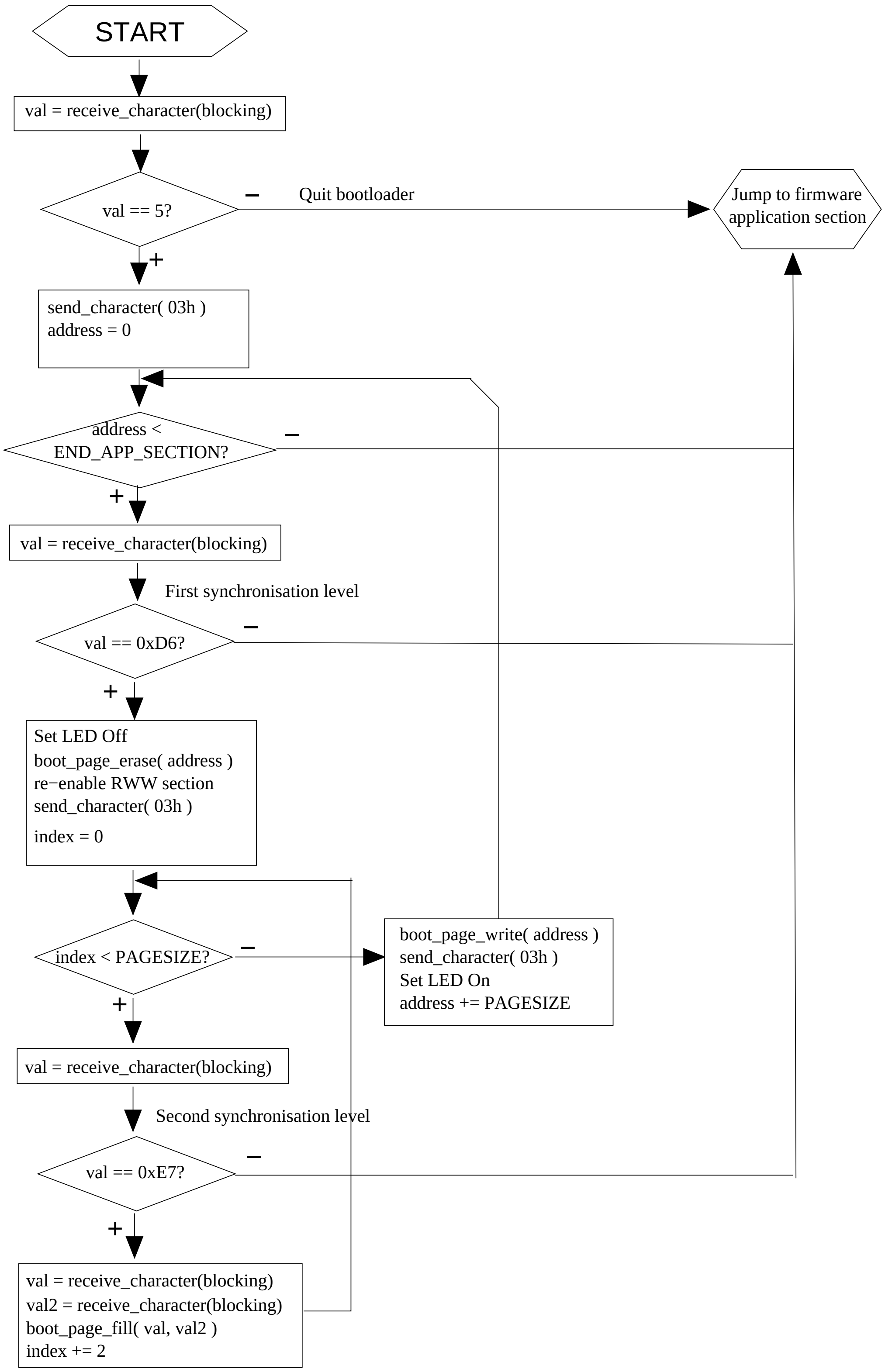
Current firmware provides a bootloader feature. By means of bootloader feature, the user can upload a new firmware release using USB cable and an application software that is provided with the EMDB409 Reader.

Bootloader allows an upload of application part only. It is not possible to upload the bootloader itself.

Bootloader is activated either on firmware start-up either by Bootloader Mode command (F3h). Start-up firmware activation is applied so that the broken (application part) firmware or firmware which does not implement Bootloader Mode command (F3h) can be uploaded. Bootloader is not activated by watch-dog reset.

Firmware data being sent to the bootloader are synchronised in two levels; hand-shake page synchronisation = 0xD6 sent twice per page, and byte synchronisation = 0xE7 sent once per two bytes (see figure on the next page). The application may transmit a next page data only if it receives the first bootloader page synchronisation byte = 0x03 (i.e.; hand-shake), and may not send the next page synchronisation byte until it receives the second bootloader synchronisation byte = 0x03 (after the bootloader performed the eeprom_page_write operation). The byte synchronisation is not applicable as the bootloader byte processing is hidden in byte reception latency.
Current Bootloader uses the same communication parameters as the application part. However, the communication parameters may differ in future.

Note: Two page synchronisation bytes apply starting from firmware release 0.7. Previous releases use one page synchronisation byte only, therefore they are not compatible. Upload of the new firmware is still possible by using original old application software until the new bootloader is uploaded using the programming cable.


START
val = receive_character(blocking)
val == 5?
–
Quit bootloader
Jump to firmware application section
+
send_character(03h)
address = 0
address < END_APP_SECTION?
–
+
val = receive_character(blocking)
First synchronisation level
val == 0xD6?
–
+
Set LED Off
boot_page_erase(address)
re−enable RWW section
send_character(03h)
index = 0
index < PAGESIZE?
–
+
boot_page_write(address)
send_character(03h)
Set LED On
address += PAGESIZE
val = receive_character(blocking)
Second synchronisation level
val == 0xE7?
–
+
val = receive_character(blocking)
val2 = receive_character(blocking)
boot_page_fill(val, val2)
index += 2

4. Obsolete product support

EMDB409 firmware supports the transponders that are already marked as obsolete products;

Transponder family	Command set support	Coding and data rate support
EM4005/EM4105	Animal mode - Read UID	Bi/32
EM4100/EM4102	Read Only mode - Read UID	Mn/32, Mn/64, Bi/32, Bi/64
EM4150/EM4350/EM4550	All	Mn/64, Mn/32
EM4469	All	Mn/(32-64), Bi/(32-64)
EM4026	Send Code ID Free-running scan Switch off/Slow down scan	Mn/32

4.1. PC to reader (Command)

PC to reader	Serial Data Bytes sent on UART											
Command	0	1	2	3	4	…					xx-1	xx
EM4005/EM4105 commands												
Single Read UID	See Animal mode – Read UID command (11h)											
EM4100/EM4102 commands												
Autodetect Read UID	See Read Only mode – Read UID command (10h)											
EM4150/EM4350/EM4550 commands												
All	See EM4450 command set											
EM4026 commands												
Send Code ID	02h	06h	50h	05h	SM	00h	CHK	03h				
Single Scan	02h	06h	51h	05h	SM	00h	CHK	03h				
Scan	02h	06h	52h	05h	SM	00h	CHK	03h				
EM4x69 commands												
Read Block	02h	04h	80h	Addr	CHK	03h						

PC to reader	Serial Data Bytes sent on UART											
Write Block	02h	08h	81h	Adrr	LSB <4 Bytes> MSB new value			CHK	03h			
New Password	02h	08h	81h	02h	LSB <4 Bytes> MSB new password value			CHK	03h			
Protection	02h	08h	81h	03h	LSB <4 Bytes> MSB protection value			CHK	03h			
Configuration	02h	08h	81h	04h	LSB <4 Bytes> MSB configuration value			CHK	03h			
Login	02h	07h	82h	LSB <4 Bytes> MSB current password value			CHK	03h				
Disable	02h	03h	83h	80h	03h							

4.2. Reader to PC (Response)

C to reader	Serial Data Bytes sent on UART											
Command	0	1	2	3	4	…					xx-1	xx
EM4x69 commands												
Read Block ACK = 00h	02h	09h	80h	00h	Addr	LSB <4 Bytes> MSB value on address Addr.			CHK	03h		
Read Block ACK ≠ 00h	02h	09h	80h	ACK	Addr	<4 Bytes> 00h 00h 00h 00h			CHK	03h		
Write Block	02h	04h	81h	ACK	CHK	03h						
New Password	02h	04h	81h	ACK	CHK	03h						
Protection	02h	04h	81h	ACK	CHK	03h						
Configuration	02h	04h	81h	ACK	CHK	03h						
Login	02h	04h	82h	ACK	CHK	03h						
Disable	02h	04h	83h	ACK	CHK	03h						
EM4026 command												
Send Code ID ACK = 00h	02h	0Eh	50h	00h	MSB <6 Bytes> LSB value of UID			2Bytes CRC	2Bytes 00h	CHK	03h	

C to reader	Serial Data Bytes sent on UART											
Send Code ID ACK ≠ 00h	02h	0Eh	50h	ACK	MSB <6 Bytes> LSB 00h			2Bytes 00h	2Bytes 00h	CHK	03h	
Single Scan ACK = 00h	02h	xx-1	51h	00h	6Bytes UID1	2Bytes CRC1	…	6Bytes UIDn	2Bytes CRCn	CHK	03h	
Single Scan ACK ≠ 00h	02h	04h	51h	ACK	CHK	03h						
Scan ACK = 00h	02h	Num	52h	00h	6Bytes UID1	2Bytes CRC1	…	6Bytes UIDn	2Bytes CRCn	CHK	03h	
Scan ACK ≠ 00h	02h	04h	52h	ACK	CHK	03h						

Note:

- All values are in a hexadecimal format
- LSB, MSB - low endian bytes ordering
- LBR, FBR - Last/First Block Read

4.3. Command description

4.3.1. Send Code ID (50h) - EM4026

After reception of this command the reader sends SEND CODE ID command and then the reader receives UID number from the transponder and sends answer to the Application software.

Possible error codes: 34h

4.3.2. Single Scan (51h) - EM4026

After reception of this command the reader receives UIDs from transponders placed on the reader during the Maximum initial random Delay time. Then the reader sends answer to the Application software.

Possible error codes: 34h

4.3.3. Scan (52h) - EM4026

After reception of this command the reader starts the automatic scan of UIDs from transponders placed on the reader during the Maximum initial random Delay time. All the UIDs found during one Delay time period are returned. After transmitting the response to the PC, the reader continues scanning. The scan process is defined by scan mode (SM) parameter; 00h for free scan, or 01h for slow-down/switch-off scan. When the PC repeats the Scan (52h) command with the same SM parameter, the firmware returns already buffered found UIDs immediately. To stop automatic scan process, invoke the Scan command with SM = FFh parameter (automatic scan process is stopped and the last buffered UIDs are returned).

Possible error codes: 34h

4.3.4. Read Block (80h) - EM4469

After reception of this command the reader sends command data bits of Read Word command and address bits of the reading word. Then the reader waits for processing pause time (tpp). Upon tpp the reader receives answer from the transponder and sends answer to the Application software.

Possible error codes: 0Bh, 10h, 12h, 13h.

4.3.5. Write Block (81h) - EM4469

After reception of this command the reader sends command data bits of Write Word command, address bits of the write word and new value of the write word. Then the reader waits for EEPROM programming time (t_{Wee}) + Initialization after Write Word time (t_{INI}). Upon t_{Wee} + t_{INI} the reader receives answer from the transponder and sends answer to the Application software.

Possible error codes: 0Bh, 10h, 12h, 13h, 15h.

4.3.6. New Password (81h) - EM4469

New Password command has the same running as Write Block (81h) command. The address of the write word is fixed (= 2) and new value of the writing word = new password value.

Possible error codes: 0Bh, 10h, 12h, 13h, 15h.

4.3.7. Protection (81h) - EM4469

Protection command has the same running as Write Block (81h) command. Difference is in the address of the writing word = 3 and new value of the writing word = new value of the protection word.

Possible error codes: 0Bh, 10h, 12h, 13h, 15h.

4.3.8. Configuration (81h) - EM4469

Protection command has the same running as Write Block (81h) command. Difference is in the address of the writing word = 4 and new value of the writing word = new value of the configuration word.

Possible error codes: 0Bh, 10h, 12h, 13h, 15h.

4.3.9. Login (82h) - EM4469

After reception of this command the reader sends command data bits of Login command and actual password value. Then the reader waits for processing pause time (tpp). Upon tpp the reader receives answer from the transponder and sends answer to the Application software.

Possible error codes: 0Bh, 10h, 12h, 13h.

4.3.10. Disable (83h) - EM4469

After reception of this command the reader sends command data bits of Disable command. The EM4469 or EM4569 accepts disable command only when the Disable bit in Tag Special Bits is set to 1. When the Disable command is accepted, the EM4469 or EM4569 stops all operations until next power-up. In case the Disable command is not accepted, EM4469 or EM4569 returns in Default Read mode.

Possible error codes: 0Bh, 12h, 13h