Application Note

EHAG 125 kHz Multitag Reader Module
ME-H10101xx

Firmware: 0.12b

4/9/2004

ELECTRONIC HARDWARE AG
Industriestr. 8 8618 Oetwil am See
T: +41 43 844 94 00 info@ehag.ch
F: +41 43 844 94 01 www.ehag.ch

Table of Content

1 Scope 2
2 Definitions and abbreviations 3
2.1 Definitions 3
2.1.1 Hex notation 3
2.1.2 ASCII notation 3
2.2 Abbreviations 3
3 Tag organization 4
3.1 Overview of supported labels 4
3.2 EM4x02 4
3.3 EM4x50 4
3.3.1 Memory organization 4
3.4 Hitag 1 6
3.4.1 Memory organization 6
3.5 Hitag 2 Memory Organization 7
3.5.1 Memory organization 7
3.6 ISO FDXB 8
3.6.1 Decoding FDXB 8
4 Hardware 10
4.1 Pin out of OEM Module 10
4.1.1 Pin out of J1 10
4.1.2 Pin out of J2 11
4.1.3 Electrical characteristics of PINs 11
5 Software 12
5.1 ASCII Protocol 12
5.2 Reader function overview 12
5.3 Instruction Set 13
5.3.1 Overview 13
5.3.2 Error Codes 13
5.3.3 Reset 14
5.3.4 Get Version 14
5.3.5 Continuous Read 15
5.3.6 Login 16
5.3.7 Read page 17
5.3.8 Write page 18
5.3.9 Set LED 19
5.3.10 Antenna power off 20
6 Timing 21
7 Frequently Ask Questions 22
7.1 Getting started 22
7.2 Release notes 22
7.2.1 Version 0.12b 22
8 References 23

1 Scope

The EHAG 125 kHz Multitag OEM Reader Module is a read write device that supports a wide range of 125 kHz tags. It supports Hitag 1 and 2, EM 4x02, EM4x50 and ISO FDXB. Using an external antenna and a serial interface it can be easily connected to a host or PC.
The Plug and Play module includes an antenna and RS232 serial interface.

The first part of the manual describes general functions and memory management of several supported tags. A listing of the memory map is given if necessary.

The second part gives a detailed description of the pin out and the electrical characteristics of the OEM module.

The third part lists the reader command set. Each command is explained in detail and an example illustrates the usage. FAQs highlight general issues using the EHAG 125 kHz Multitag OEM Reader Module.

Appendices describes the Plug and Play Module, its pin out and 12 V power supply. Appendix B introduce to the customized antenna design. A standard layout is listed as reference.

2 Definitions and abbreviations

2.1 Definitions

2.1.1 Hex notation

A hexadecimal value is noted with a following h, i.e. A1h has the value A1 hexadecimal.

2.1.2 ASCII notation

ASCII characters are listed within apostrophes, i.e. ‘x’ means a decimal based value x

2.2 Abbreviations

LSB	Least significant bit
MSB	Most significant bit
RFU	Reserved for future use

Figure 2-1: Abbreviations

3 Tag organization

3.1 Overview of supported labels

Tag	SN	Read page	Write page	Properties
EM4x02	√	-	-	5 bytes read only
EM4x50	√	√	√	32 x 4 bytes r/w, password
HITAG1	√	√	√	64 x 4 bytes r/w
HITAG2	√	√	√	7 x 4 bytes r/w, password
ISO - FDXB	√	-	-	8 bytes read only

Figure 3-1: Supported labels

3.2 EM4x02

The EM4x02 label only provides a 5 byte serial number. The label start to send its response immediately after entering an energizing field. Each transponder has its own unique serial number which cannot be changed. For further information refer to [1]

3.3 EM4x50

The EM4x50 has 1 kbit of EEPROM memory which is organized in 32 pages of each 4 bytes. The tag supports a password to protect its configuration settings. The UID and the Identification number are laser programmed at the manufacturing process and are read only. All other data is set to 0 as default.
For further information refer to [2]

3.3.1 Memory organization

Page	Function	Access
00h	Password	write access
01h	Protection word	Password protected
02h	Control word	Password protected
03h - 1Fh	User memory	Read / write
20h	Device serial number	read only
21h	Device identification	read only

Figure 3-2: Memory organization of EM4x50

3.3.1.1 Password

The password is read protected. A user has to log in before he can change page 00h – 02h.
The password is set to 00000000h as default.

3.3.1.2 Protection word

Protection word (01h)			
Bit 31 - 24	Bit 23 - 16	Bit 15 - 8	Bit 7 - 0
End WI	Start WI	End RP	Start RP

Figure 3-3: Protection word

The protection word is divided into two parts. First part (bit 0, bit 15) specifies the read protection (RP) area.
Bit 16 to bit 31 defines the area of the write inhibited (WI) pages.
Write access to the protection word needs a previous log in.

3.3.1.3 Control word

Control word (02h)		
Bit 31 - 17	Bit 16	Bit 15 - 0
RFU	PWC on/off	RFU

Figure 3-4: Control word

The password check (PWC) at bit 16 defines the write access to the user area (03h – 1Fh). If it is set a successful log in prior to any write process is mandatory. It does not affect write access to the control word and protection word.

3.3.1.4 User memory

The user memory is free to use. Write access depends on password check bit (control word) and write inhibited area of the protection word.
If the PWC is set a log in previous to any write command is mandatory.

3.3.1.5 Device serial number, device identification

These two pages are read only and defined at the manufacturing process. They are stored in a specific area of the tag. Page 20h (device serial number) is returned if a tag is selected.

3.4 Hitag 1

Hitag 1 has 2 kbit EEPROM memory. The memory is organized in 48 pages. Each page consists of 4 bytes. For further information see [3].

3.4.1 Memory organization

Page	Function	Access
00h	Serial number	Read only
01h	Configuration word	Read / write
02h – 0F	RFU	Not accessable
10h – 3Fh	User data	Read / write

Figure 3-5: Hitag 1 memory organization

3.4.1.1 Serial number

The serial number is factory programmed and cannot be changed anymore. It is used to distinguish Hitag 1 tags from each other.

3.4.1.2 Configuration word

The configuration word holds information about the tag formatting. Do not alter the contents. Invalid data might inhibit a tag for further operation.

3.4.1.3 User data

User data is free for use.

3.5 Hitag 2 Memory Organization

Hitag 2 tags have 256 bits EEPROM which is divided into 8 pages. Each page consists of 4 bytes. The tag is only supported in password mode [4].

3.5.1 Memory organization

Page	Function	Access
00h	Serial number	Read only
01h	Password RWD	Read / write
02h	RFU	Read only
03h	Configuration page	Read / write
04h – 07h	User data	Read / write

Figure 3-6: Hitag 2 memory organization

3.5.1.1 Serial number

The serial number is factory programmed and cannot be changed anymore. It is used to distinguish Hitag 2 tags from each other.

3.5.1.2 Password RWD

The password RWD and the Password TAG (see Configuration page 03h) is used during the mutual authentication process. Changes of the password needs a new authentication.
Default value is 4D494B52h.

3.5.1.3 Configuration

The Configuration page sets up a tag. The reader only supports password mode. All other modes will not be detect from the reader.

Configuration page (03h)			
Byte 3	Byte 2	Byte 1	Byte 0
RFU	Password TAG		

Figure 3-7: Configuration page

The password TAG is used during the authentication. See above Password RWD.

3.5.1.4 User data

User data is free for use.

3.6 ISO FDXB

The ISO FDXB tag only provides a 8 byte serial number. The tag starts automatically sending its ID number after entering an energizing field. The data is stored LSB first.

3.6.1 Decoding FDXB

The data format of the ISO FDXB tag is coded as described below. The serial number is divided into three parts: application ID, country code, national ID.

ISO FDXB							
Byte 7	Byte 6	Byte 5	Byte 4	Byte 3	Byte 2	Byte 1	Byte 0
National ID					Country code	Application ID	

Figure 3-8: ISO FDXB

3.6.1.1 Preparing data

Following steps must be done prior to any interpretation of the serial number.

- Cut off the first character to get the 8 byte serial number
- First the data stream has to be reversed. LSB takes place in the end and MSB is first.
- Reverse each nibble.

3.6.1.2 Application ID

The Application ID specifies the application of the transponder.

3.6.1.3 Country code

The country code only consists of 12 bits (byte 2 and low nibble of byte 3). Decoding of the country code is done as follows:

- Shift right two times.
- Convert the hexadecimal number to decimal based number

3.6.1.4 National ID

The national ID is unique for each country. The national ID consists of 36 bits (byte 7, byte 6 , byte 5 , byte 4, high nibble of byte 3)
Decoding is done simply by converting the number from hexadecimal system to decimal based numbers.

3.6.1.5 Example

The example shows the correct decoding of an ISO FDXB transponder.

Data	**Comments**
70 91 53 12 EA 6F 00 01h	Number received from the reader
10 00 F6 AE 21 35 19 07h	Reversed number
80 00 F6 57 48 CA 89 0Eh	Reverse each nibble
8000h	Application Identifier
F65h	Country code
3D9h	2 times right shift
‘985’	Convert to decimal based number
748CA890Eh	National ID
‘31286003982’	Convert to decimal based number

Figure 3-9: ISO – FDXB decoding example

4 Hardware

4.1 Pin out of OEM Module

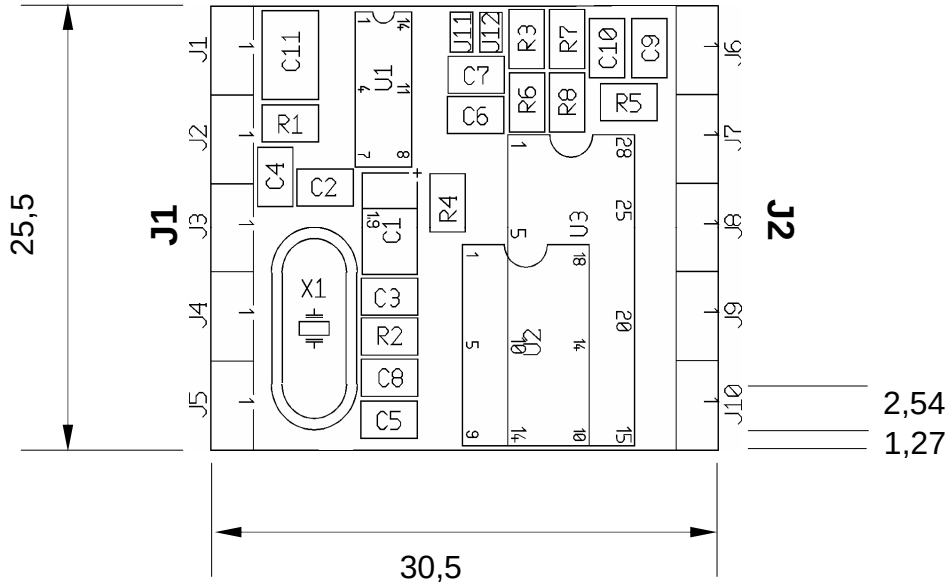

Figure 4-1: Pin out of the reader device

4.1.1 Pin out of J1

PIN	PIN Nr	Description
ARX	1	Antenna RX
ATX	2	Antenna TX
VDD	3	+5 V DC
GND	4	Ground
RFU	5	Reserved for future use
RFU	6	Reserved for future use
RFU	7	Reserved for future use
RFU	8	Reserved for future use
RFU	9	Reserved for future use
RFU	10	Reserved for future use

Figure 4-2: Pin out of jumper 1

4.1.2 Pin out of J2

PIN	PIN Nr	Description
VDD	20	+5 V DC
GND	19	Ground
LEDg	18	LED green (reading LED)
LEDr	17	LED red
EN	16	Enable reader
RFU	15	Reserved for future use
RFU	14	Reserved for future use
RFU	13	Reserved for future use
TX	12	TX to PC
RX	11	RX from PC

Figure 4-3: Pin out of jumper 2

4.1.3 Electrical characteristics of PINs

PIN	PIN Nr	Voltage	Current (max)	Description
RX TX	11 12	USART[1]	-	To RS232, RS485 device driver
EN	16	ST[2]	25 mA	High will disable the reader device
LEDr	17	GND	25 mA	Logic Low, used for LED
LEDg	18	LED	25 mA	With 330 Ω (internal)
ARX ATX	1 2	(depends on antenna tuning)	200 mA_{PP}	Antenna input Antenna output
RFU	5,6,7,8, 9,10,13, 14,15	-	-	Not connected
GND	4,19	GND	-	Supply Ground
VDD	3,20	+5 V DC	150 mA	Supply Voltage

Figure 4-4: Electrical characteristics of pins

[1] Universal Synchronous Asynchronous Receiver Transmitter
[2] Schmitt trigger buffer output

5 Software

5.1 ASCII Protocol

As a default data is transmitted at 9600,n,8,1. This protocol is designed for easy handling. The commands can be issued using a terminal program. Data is transmitted as ASCII hexadecimal that can be displayed on any terminal program (e.g. HyperTerminal).

Command	Data
Various length	Various length

Figure 5-1: ASCII protocol frame

5.2 Reader function overview

The reader device provides an easy interface. Each time a card has to be selected before a read or write command can be applied.
The reader does not provide an own select command. The continuous read command searches for a tag within the antenna field. If a tag is found the serial number is returned. A card can only be accessed correctly after the continuous read command has detected the card successfully.
The continuous read command does not stop automatically. The user has to send a character to the reader to stop the continuous read command.
Since the continuous read command does not return an error code in any case of failure a timeout must be implemented. Sending a command the continuous read command is canceled. The reader sends back the response ('S').
Following figure describes the correct command sequence issued to a tag.

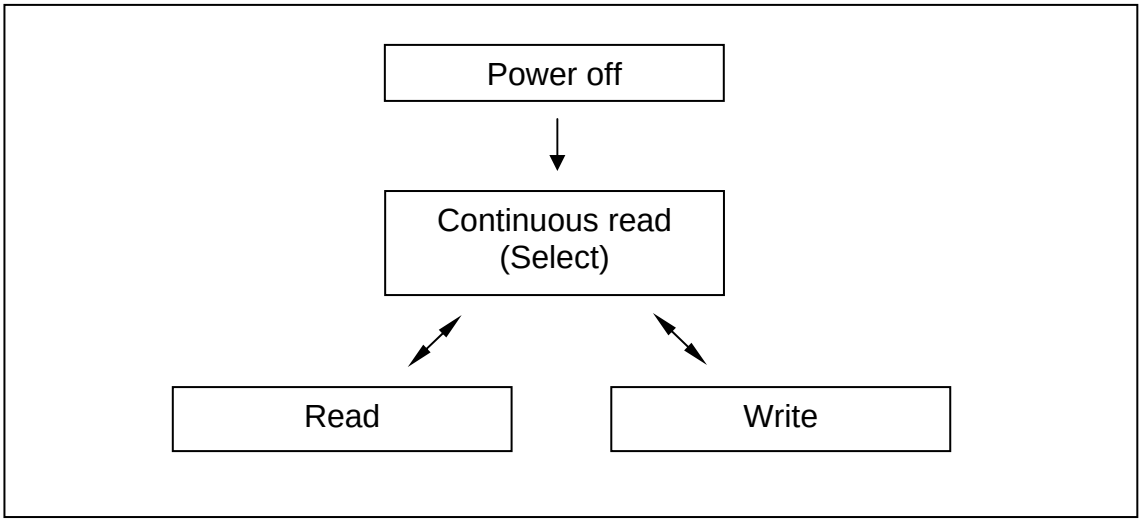

Figure 5-2: Reader function overvew

5.3 Instruction Set

Following table describes all commands of the reader device. Each command returns an answer to the host. Exceptions are mentioned explicitly. The green LED is acknowledging a successfully executed command.

5.3.1 Overview

Command	Description
‘x’, ‘z’	Reset
‘v’	Get version
‘c’	Continuous read
‘l’	Login
‘r’	Read page
‘w’	Write page
‘p’	Antenna power off

Figure 5-3: Command overview

5.3.2 Error Codes

Following figure shows an overview of all error messages of the reader device.

Error Code	Description
‘?’	Unknown command
‘N’	Command was not performed successfully
‘S’	Continuous read stopped

Figure 5-4: Error codes

5.3.3 Reset

This command executes a power on (software) reset. This command will reset the reader module as well as all tags in the antenna field.

5.3.3.1 Command

Command	Data
‘x’, ‘z’	none

5.3.3.2 Answer

Answer	Description
none	“MULTITAG 0.12b” + CR + LF

5.3.3.3 Start up

The reader starts up in continuous read mode. The firmware string is not returned.

5.3.3.4 Reset Timing

The power up timing depends on environmental conditions such as voltage ramp up. For handheld devices the timing may depend on the charging state of the battery.

5.3.4 Get Version

This command returns the current version string of the reader module.

5.3.4.1 Command

Command	Data
‘v’	none

5.3.4.2 Answer

Answer	Description
none	“MULTITAG 0.12b ” + CR + LF

5.3.4.3 Example

Command	Description
v	MULTITAG 0.12b Version of the reader module

5.3.5 Continuous Read

The reader device reads and displays the serial numbers continuously while a tag remains in the field. This command stops if any character is sent to the reader module.
Only one tag type is detected at the same time. The reader supports different tag types. Though a single continuous read instruction needs a short time.

5.3.5.1 Command

Command	Data
'c'	none

5.3.5.2 Answer

Answer	Description
data	Leading character (1 byte) + serial number (n bytes)

Number of bytes depends on tag type.
This command is not supported in binary protocol mode.

5.3.5.3 Leading character

The leading character specifies a single tag type. It can be used to determine the present tag type and control tag specific commands. Cards have different UID length, i.e. ISO FDXB cards use an 8 byte UID whereas Hitag 1 and Hitag 2 cards only 4 bytes.
Following table describes all leading characters of supported tag types.

Tag type	UID length	Description
'h'	4 bytes	Hitag 1
'H'	4 bytes	Hitag 2
'T'	4 bytes	EM 4x50
'U'	5 bytes	EM4x02
'Z'	8 bytes	ISO FDXB

Figure 5-5: Leading character of continuous read mode

5.3.5.4 Remarks

ISO FDXB tags have increased serial numbers in plain mode. Plain mode serial numbers have 10 bytes.

5.3.5.5 Simple access control applications

Serial numbers are not encrypted and always sent plain to the reader. This results in a low-level security application.

5.3.6 Login

The login is needed to authenticate to Em4x50 and Hitag 2 tags. It is mandatory prior to any read write access to pages. Login with default keys is done automatically. Last detect tag type is used for login.

5.3.6.1 Command

Command	Data
'l'	Password (4 bytes)

5.3.6.2 Answer

Answer	Description
'L'	Login succeeded
'N'	Error: Login failed. Key is wrong or card removed

5.3.6.3 Example

Command	Description
L01234567	L Login has succeeded.

5.3.7 Read page

This command reads one data block of a card. Size of returned data depends on the used tag. A valid page address depends on the present tag. Page read on page 00 returns the serial number of EM4x02 and ISO FDXB tags.

5.3.7.1 Command

Command	Data
'r'	page address (1 byte)

5.3.7.2 Answer

Answer	Description
data	page data (depends on tag type)
'N'	Error: No tag in field

5.3.7.3 Page data

Following table describes the default page sizes.

Tag type	Page size	Description
Hitag 1	4	48 pages
Hitag 2	4	8 pages
EM4x05	4	32 pages
EM4x02	-	Only page 00h
ISO FDXB	-	Only page 00h

Figure 5-6: page data

5.3.7.4 Remarks

EM 4x02 and ISO FDXB supports only serial numbers. Reading page 00h will return the UID of the tag.

5.3.7.5 Read failure 'N'

This error is displayed if the reader receives bad data. Additionally this error is generated if a page is read which is not physically located on the card.

5.3.7.6 Examples

r05	00112233 reads page 05. page data is 00112233

5.3.8 Write page

This command writes data to a page. A read after write is done automatically to ensure correct writing. Not all tags supports writing.

5.3.8.1 Command

Command	Data
‘w’	page address (1 byte) + data (n bytes)

5.3.8.2 Answer

Answer	Description
data	‘w’ + page data (depends on tag type)
‘N’	Error: write failure

5.3.8.3 Page data

Following table describes the default page sizes.

Tag type	Page size	Description
Hitag 1	4	Accessible pages according memory organization
Hitag 2	4	Accessible pages according memory organization
EM4x05	4	Accessible pages according memory organization
EM4x02	-	Not supported
ISO FDXB	-	Not supported

Figure 5-7: page data

5.3.8.4 Write failure ‘N’

This error is displayed if bad transmission conditions are given. If the page address exceeds the physical number of pages of a tag this error is thrown too.

5.3.8.5 Example

Command	Description
w0511223344	w11223344 writes data 11223344 on page 05.

5.3.9 Set LED

This command controls the LED. The user can set the state of the LED manually.

5.3.9.1 Command

Command	Data
‘d’	LED state (1 byte)

5.3.9.2 Answer

Answer	Description
none	String of LED state

5.3.9.3 LED

Command	Answer	Description
‘dg’	DG	Switch on LED green, LED red off
‘dr’	DR	Switch on LED red, LED green off
‘dn’	DN	Switch off both LEDs

Figure 5-8: LED response

5.3.9.4 Examples

Command	Description
dr	DR Switch on LED red

5.3.10 Antenna power off

This command switches off the antenna power.

5.3.10.1 Command

Command	Data
‘p’	Reader enters the stand by mode

5.3.10.2 Answer

Answer	Description
‘P’	Positive acknowledge

5.3.10.3 Power off

The reader enters the stand by mode. Power consumption is decreases. All tags in the antenna field are powered off and reset. The stand by mode is only entered manually.
To switch off the whole unit pin 16 (Enable) has to set to logic low.

5.3.10.4 Power on

Power on is only performed sending a reset command (‘x’).

5.3.10.5 Example

Command	Description
P	P Reader enters stand by mode

6 Timing

Following table describes the timing of the EHAG 125 kHz Multitag Reader Module.

Command	$Time_{Fail}$	$Time_{Typ}$	$Time_{Max}$
	[ms]	[ms]	[ms]
Reset [3]			
Power up	-	148,0	290,0
Software (x)	-	176,0	344,0
Get version (v)	-	0,14	-
All	-	46,0	90,0
Hitag 1	-	69,2	70,5
Hitag 2	-	25,2	26,5
EM4x02	-	74,0	75,5
EM4x50	-	87,2	90,0
ISO FDXB	-	46,0	56,0
Login			
Read page			
Hitag 1	24,0	71,6	73,5
Hitag 2	27,6	26,8	28,0
EM4x02	86,4	74,6	75,5
EM4x50	23,2	87,0	88,0
ISO FDXB	0,56	56,0	57,5
Write page			
Hitag 1	22,4	98,4	100,0
Hitag 2	26,4	90,5	95,2
EM4x02	0,26	-	-
EM4x50	51,2	174,0	175,5
ISO FDXB	0,46	50,5	56,8
Antenna off	-	0,24	-
Unknown command	0,14	-	-

[3] Reset will cause an error if reader IC Initialization fails

7 Frequently Ask Questions

7.1 Getting started

To test and interface the EHAG 125 kHz Multitag OEM Reader Module, no sophisticated µP development system is needed. All you need is a PC, a connection cable and a power supply for the reader. If you are using Microsoft Windows (98/NT/2000/XP,…), take following steps:

1. Make sure, that your reader is RS232-interface type
1. Start HyperTerminal
2. Create a new connection (FILE/NEW CONNECTION)
3. Enter a name of connection
4. Choose connect COM2 (COM1) direct connection
5. Communication settings: 9600,8,n,1,no handshake
6. Connect the reader to COM2 (COM1) of the PC and apply appropriate the supply voltage (+5V as default). The reader sends a string to the PC (i.e. “MULTITAG 0.12b”). This string identifies the firmware of the reader module.
7. Put a tag to your reader. Serial numbers should be displayed properly
8. Enter commands via the keyboard. They are transmitted to the reader and the reader replies with its response.

If using an operating system different from Microsoft Windows you may use any other terminal program which is capable of receiving/transmitting via the serial port of your PC.

7.2 Release notes

7.2.1 Version 0.12b

7.2.1.1 Bug fixes

- EM4002 is fully supported

8 References

[1] EM4102 transponder product description, Rev. B/273, EM Microelectronic-Marin SA, 1999

[2] EM4150 transponder product description, 6/99 Rev/626, EM Microelectronis-Marin SA, 1999

[3] Hitag 1 Transponder family documentation, Product Specification Revision 2.2, Philips, January 1999

[4] Hitag 2 Transponder family documentation, Product Specification Revision 2.1, Philips, October 1997