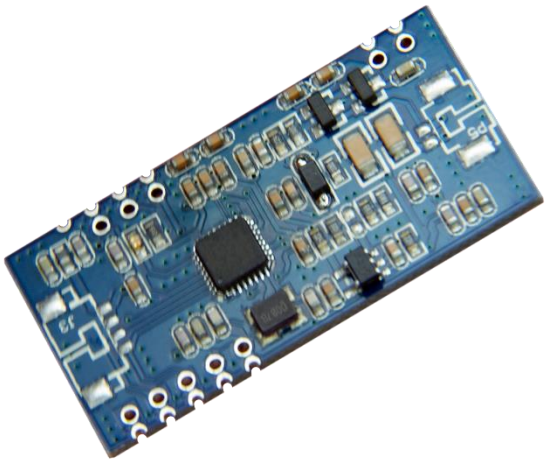

OEM LF1S Devices
LF RFID OEM Module
Communication Protocol
Tag Types: Read-only, Hitag 1, Hitag S, FDX-B, ID Card

Date	Version	Description
2018-09-04	5.1	Layout changed, updated to newer FW version that combined Hitag 1 with Hitag S, removed Hitag 2, added further tag types
2020-12-17	5.1a	Data tag information added, some command examples exchange with tested telegrams, examples added
2021-03-31	5.1a	Typos fixed

Contents

1 Protocol Description

1.1 Default Baudrate

Baudrate	Data Bits	Start Bits	Stopp Bits	Checksum
9600 bps	8	1	1	None

1.2 Data Package Format

Data package format, command package is sent from Host to Reader, response package returned from Reader to Host

CMD package format (Host to Reader)

STX	STATION ID	DATA LENGTH	CMD	DATA [0..N]	BCC	ETX

(BCC) = STATION ID ⊕DATALENGTH⊕ CMD⊕ DATA [0] ⊕ … ⊕ DATA [n], where ⊕ is the “EOR”.

Response package format (Reader to Host)

STX	STATION ID	DATA LENGTH	STATUS	DATA[0..N]	BCC	ETX

(BCC) = STATION ID ⊕DATA LENGTH⊕ STATUS⊕ DATA [0] ⊕ … ⊕ DATA [n], where ⊕ is the “EOR”.

1.3 Byte Description in Data Package

Field	Length	Description	Remark
STX	1	0xAA: ‘start byte’ – standard control byte, means the start of one data package.	0xAA = 0b1010.1010
STATION ID	1	Device address, necessary in multiple device communicating, when reader receive data package, it will judge the inner address if match up with itself preset, only response when match up	Address 0x00 is the special address only used under Single mode, reader will response any data package with 0 address(no address judge).
DATALENGTH	1	Data byte length in data package, including CMD/STATUS and DATA field, but no BCC. LENGTH= numbers of byte (CMD/STATUS + DATA[0..N])	
CMD	1	Command byte: compose with one Cmd byte	Only used in Send package
STATUS	1	Return status byte: status return from Reader to Host	Only used in Return package
DATA [0-N]	0–241	This is a data flow related to Length and CMD byte. Some part of commands no need additional data	
BCC	1	8bits checksum byte, including all bytes XOR checksum besides STX, ETX	
ETX	1	0xBB: ’ stop byte’ – standard control byte, means end of data package	0xBB = 0b1011.1011

1.4 Command List

CMD	Name	Description
System Commands		
0x51	Get_VersionNum	To get device hardware version number
0x52	BUZ_control	Buzzer control
0x53	LED_control	LED control
0x54	SET_ANT	To open or close antenna
Command for read-only Data Tags		
0x57	EM4100/4200_GetUID	Get UID from read-only tag
Commands for Hitag-1 + Hitag S Data Tags		
0x58	Hitag1/S_Request	Request card
0x59	Hitag1/S_Select	Select card
0x5C	Hitag1/S_Quiet	Card quiet
0x5A	Hitag1/S_ReadPage	Read data per page
0x5B	Hitag1/S_WritePage	Write data per page
0x60	Hitag1/S_LockPage	Lock page
Commands for further Data Tags		
0x56	Read FDX-B	Read FDX_B Data Tag (ISO11784/85)
0x5D	Format to FDX-B	Format Hitag S Tag for operation as an FDX-B
0x5E	Format to ID Card	Format Hitag S Tag for operation as an ID Card

IMPORTANT NOTE

Only Modules with Designation LF1S support Hitag 1 + Hitag S.

2 Command Examples

2.1 General

This chapter is intended to provide an easy start with these RFID devices. Is shows only a few commands that are explained in detail. For full reference to all commands, please consult the rest of this manual.

2.2 Communication Parameters

- 9600 Baud
- 8 data bits
- 1 start bit
- 1 stop bit
- no parity
- no flow control

2.3 Checksum Calculation

Checksum is calculated as XOR over these parts of a telegram:

- Device Address
- Payload Length Information
- Command Code (Payload)
- Parameters (Payload)

2.4 Command Examples

2.4.1 Get Firmware Version Information

Command from PC/PLC to RFID device:

AA 00 01 51 50 BB

The Bytes in Detail:

AA	= Start of Telegram
00	= Device Address, 0x00 = all devices react
01	= Payload Length
51	= Command Code (Counted as Payload)
50	= Checksum
BB	= End of Telegram

Reply from RFID device to PC/PLC:

AA 00 07 00 48 69 74 61 67 53 07 BB

The Bytes in Detail:

AA	= Start of Telegram
00	= Device Address, 0x00 = all devices react
07	= Payload Length
00	= Status, 0x00 = OK (Payload)
48 69 74 61 67 53	= Firmware Version Information, "HitagS" (Payload)
07	= Checksum
BB	= End of Telegram

2.4.2 Read UID of Read-Only RFID Tag

Command from PC/PLC to RFID device:

AA 00 01 57 56 BB

The Bytes in Detail:

AA	= Start of Telegram
00	= Device Address
01	= Payload Length
57	= Command Code (Payload)
56	= Checksum
BB	= End of Telegram

Reply from RFID device to PC/PLC:

AA 00 06 00 01 10 2F BB AA 29 BB

The Bytes in Detail:

AA	= Start of Telegram
00	= Device Address
06	= Payload Length
00	= Status, 0x00 = OK
01 10 2F BB AA	= UID, 5 Bytes
29	= Checksum
BB	= End of Telegram

2.4.3 Read UID of Hitag1/S Tag

Command from PC/PLC to RFID device:

AA 00 01 58 59 BB

The Bytes in Detail:

AA	= Start of Telegram
00	= Device Address
01	= Payload Length
58	= Command Code (Payload)
59	= Checksum
BB	= End of Telegram

Reply from RFID device to PC/PLC:

AA 00 05 00 C5 0F 4A 8E 0B BB

The Bytes in Detail:

AA	= Start of Telegram
00	= Device Address
05	= Payload Length
00	= Status, 0x00 = OK
C5 0F 4A 8E	= UID, 4 Bytes
0B	= Checksum
BB	= End of Telegram

2.4.4 Select Hitag1/S

Before you can read/write data you need to select the tag first:

Command from PC/PLC to RFID device:

AA 00 05 59 C5 0F 4A 8E 52 BB

The Bytes in Detail:

AA	= Start of Telegram
00	= Device Address
05	= Payload Length
59	= Command Code (Payload)
C5 0F 4A 8E	= UID of tag to Select
52	= Checksum
BB	= End of Telegram

Reply from RFID device to PC/PLC:

AA 00 05 00 CA 00 00 AA 65 BB

The Bytes in Detail:

AA	= Start of Telegram
00	= Device Address
05	= Payload Length
00	= Status, 0x00 = OK
CA 00 00 AA	= Configuration word, you can use this to identify the tag exactly
65	= Checksum
BB	= End of Telegram

2.4.5 Read Data from Hitag1/S

Command from PC/PLC to RFID device:

AA 00 02 5A 00 58 BB

The Bytes in Detail:

AA	= Start of Telegram
00	= Device Address
02	= Payload Length
5A	= Command Code
00	= Page Address to Read From
58	= Checksum
BB	= End of Telegram

Reply from RFID device to PC/PLC:

AA 00 05 00 C5 0F 4A 8E 0B BB

The Bytes in Detail:

AA	= Start of Telegram
00	= Device Address
05	= Payload Length
00	= Status, 0x00 = OK
C5 0F 4A 8E	= Memory Content of Page 0, Page 0 = UID

0B = Checksum
BB = End of Telegram

3 System Commands

3.1 Get_VersionNum (0x51)

Send Data

None

Reply with Success

STATUS: 0x00 – OK
DATA[0~5]: VersionNum

Reply in Case of Error

STATUS: 0x01 – FAIL
DATA: None

Example

Command from PC/PLC to RFID device: AA 00 01 51 50 BB
Reply from RFID device to PC/PLC: AA 00 07 00 48 69 74 61 67 53 07 BB
Note: 48 69 74 61 67 53 is the hardware version number

3.2 BUZ_control (0x52)

Send Data

DATA[0]: Buzzer control time, unit as ms 0x00 … 0xFF

Reply with Success

STATUS: 0x00 – OK
DATA: None

Reply in Case of Error

STATUS: 0x01 – FAIL
DATA: None

Example

Command from PC/PLC to RFID device: AA 00 02 52 64 34 BB (BUZ beeping 100 ms)
Reply from RFID device to PC/PLC: AA 00 01 00 01 BB (confirmation)

3.3 LED_control (0x53)

Send Data

DATA[0]: LED number 0x00 = LED1
0x01 = LED2
DATA[1]: LED control time, unit as ms 0x00 … 0xFF

Reply with Success

STATUS: 0x00 – OK
DATA: None

Reply in Case of Error

STATUS: 0x01 – FAIL

DATA: None

Example

Command from PC/PLC to RFID device: AA 00 03 53 00 64 34 BB (control LED1 lighting 100 ms)
Reply from RFID device to PC/PLC: AA 00 01 00 01 BB

3.4 SET_ANT (0x54)

Send Data

DATA[0]: control flag 0x00 = close antenna
0x01 … 0xFF = open antenna

Reply with Success

STATUS: 0x00 – OK
DATA: None

Reply in Case of Error

STATUS: 0x01 – FAIL
DATA: None

Example

Command from PC/PLC to RFID device: AA 00 02 54 00 56 BB Close antenna
Reply from RFID device to PC/PLC: AA 00 01 00 01 BB
Note: reader default is antenna opened after power up

4 Command for read-only Data Tag

4.1 EM4100/4200_GetUID (0x57)

Send Data

None

Reply with Success

STATUS: 0x00 – OK
DATA[0~4]: 5byte card UID

Reply in Case of Error

STATUS: 0x01 – FAIL
DATA: None

Example

Command from PC/PLC to RFID device: AA 00 01 57 56 BB
Reply from RFID device to PC/PLC: AA 00 06 00 01 0F C3 4E 30 B5 BB, among them 01 0F C3 4E 30 is card UID

5 Hitag S Commands

5.1 Hitag1/S_Request (0x58)

Send Data

None

Reply with Success

STATUS: 0x00 – OK
DATA[0~3]: 4 byte card UID

Reply in Case of Error

STATUS: 0x01 – FAIL
DATA: None

Example

Command from PC/PLC to RFID device: AA 00 01 58 59 BB
Reply from RFID device to PC/PLC: AA 00 05 00 C5 0F 4A 8E 0B BB, among them C5 0F 4A 8E is card UID

5.2 Hitag1/S_Select (0x59)

Send Data

DATA[0~3]: card UID

Reply with Success

STATUS: 0x00 – OK
DATA[0~3]: HitagS configured package data, this is the memory contents of page 0x01 which is the configuration word

Reply in Case of Error

STATUS: 0x01 – FAIL
DATA: None

Example

Command from PC/PLC to RFID device: AA 00 05 59 31 1E 45 72 44 BB
Reply from RFID device to PC/PLC: AA 00 05 00 CA 00 00 AA 65 BB
Note: CA 00 00 AA is card configured package data

5.3 Hitag1/S_Quiet (0x5C)

Send Data

None

Reply with Success

STATUS: 0x00 – OK
DATA: None

Reply in Case of Error

STATUS: 0x01 – FAIL
DATA: None

Example

Command from PC/PLC to RFID device: AA 00 01 5C 5D BB
Reply from RFID device to PC/PLC: AA 00 01 00 01 BB ,make card enter Quiet status

5.4 Hitag1/S_ReadPage (0x5A)

Send Data

DATA[0]: page address

Reply with Success

STATUS: 0x00 – OK
DATA[0~3]: 4Byte card data

Reply in Case of Error

STATUS: 0x01 – FAIL
DATA: None

Example

Command from PC/PLC to RFID device: AA 00 02 5A 00 58 BB to read Page0
Reply from RFID device to PC/PLC: AA 00 02 5A 00 58 BB

5.5 Hitag1/S_WritePage (0x5B)

Send Data

DATA[0]: Page address
DATA[1~4]: 4Byte data

Reply with Success

STATUS: 0x00 – OK
DATA: None

Reply in Case of Error

STATUS: 0x01 – FAIL
DATA: None

Example

Command from PC/PLC to RFID device: AA 00 06 5B 3F 00 01 02 03 62 BB
Write data of 00 01 02 03 into Page 3F of HitagS 2048 card
Reply from RFID device to PC/PLC: AA FF 01 00 FE BB

5.6 Hitag1/S_LockPage (0x60)

Send Data

DATA[0]: Lock page parameter
0x01 = Lock page 1
0x02 = Lock page 2, page 3
0x03 = Lock page 4, page 5
0x04 = Lock page 6, page 7
0x05 = Lock page 8, page 9, page 10, page 11
0x06 = Lock page 12, page 13, page 14, page 15
0x07 = Lock pages 16 – 23

0x08 = Lock pages 24 – 31
0x09 = Lock pages 32 – 47
0x0A = Lock pages 48 – 63

Reply with Success

STATUS: 0x00 – OK
DATA: None

Reply in Case of Error

STATUS: 0x01 – FAIL
DATA: None

Example

Command from PC/PLC to RFID device: AA 00 02 60 01 63 BB, Lock Page 1
Reply from RFID device to PC/PLC: AA FF 01 00 FE BB

6 Commands for FDX-B Data Tags

6.1 Read FDX-B tag/card (ISO11784/85) (0x56)

Send Data

None

Reply with Success

STATUS: 0x00 – OK
DATA[0~11]: 12 Bytes card data, including 5 bytes national code + 2 bytes country code +1 byte data mark +1 byte animal tag mark+ 3 bytes customized data

Reply in Case of Error

STATUS: 0x01 – FAIL
DATA: None

Example

Command from PC/PLC to RFID device: AA 00 01 56 57 BB
Reply from RFID device to PC/PLC: AA 00 0D 00 00 00 00 00 00 00 00 01 01 00 00 00 0D BB

6.2 Format Hitag S tag into FDX-B (0x5D)

Send Data

DATA[0]: lock flag(1 byte)
DATA[1-5]: national (5 byte)
DATA[6-7]: country code (2 bytes)
DATA[8-9]: animal flag(2 bytes)
DATA[10-12]: user data (3 bytes)

Reply with Success

STATUS: 0x00 – OK
DATA: none

Reply in Case of Error

STATUS: 0x01 – FAIL
DATA: None

Example

Command from PC/PLC to RFID device: AA 00 0E 5D 00 00 00 00 00 00 00 00 01 01 00 00 00 53 BB
Reply from RFID device to PC/PLC: AA 00 01 00 01 BB

6.3 Format Hitag S cards into ID card (0x5E)

Send Data

DATA[0] : lock flag(1 byte)
DATA[1-5]: EM4100 card Serial number (5 byte)

Reply with Success

STATUS: 0x00 – OK
DATA: none

Reply in Case of Error

STATUS: 0x01 – FAIL
DATA: None

Example

Command from PC/PLC to RFID device: AA 00 07 5E 00 10 00 00 00 01 48 BB
Reply from RFID device to PC/PLC: AA 00 01 00 01 BB

7 Data Tags, Memory Layout

7.1 EM4100 (64 bit), EM4102 (64 bit), EM4200 (128 bit)

These are read-only types, so you can only read the UID here.

7.2 Hitag S2048 (2 kbit, 256 Bytes, 64 Blöcke)

Memory blocks (pages) of 32 bit/4 Bytes.

Block #	Hex-Address	Access	Description
1	00	Read-only	UID
2	01	Read/Write	Configuration word (Hitag S: CA0000AA)
3	02	No Access	—
4	03	Read/write	Configuration word, password protected, default PW: 0000 0000 h
5	04	Read/Write	Memory for user data
…	…	…	Memory for user data
64	3F	Read/Write	Memory for user data

7.3 Hitag S256 (256 bit, 32 Bytes, 8 Blöcke)

Memory blocks (pages) of 32 bit/4 Bytes.

Block #	Hex-Address	Access	Description
1	00	Read-only	UID
2	01	Read/Write	Configuration word (Hitag S: CA0000A9)
3	02	No Access	—
4	03	Read/Write	Configuration word, password protected, standard PW: 0000 0000 h
5	04	Read/Write	Memory for user data
6	05	Read/Write	Memory for user data
7	06	Read/Write	Memory for user data
8	07	Read/Write	Memory for user data

7.4 Hitag S64 (64 bit, 8 Bytes, 2 Blöcke)

Memory blocks (pages) of 32 bit/4 Bytes.

Block #	Hex-Address	Access	Description
1	00	Read-only	UID
2	01	Read/Write	Configuration word (Hitag S: CA0000A8)

7.5 Hitag 1 (2 kbit, 256 Bytes)

Memory blocks (pages) of 32 bit/4 Bytes.

Block #	Hex-Address	Access	Description
1	00	Read-only	UID
2	01	Read/Write	Configuration word (Hitag 1: FF77AA00)
3	02	No Access	—
…	…	No Access	—

16	0F	No Access	—
17	10	Read/Write	Memory for user data
…	…	…	Memory for user data
64	3F	Read/Write	Memory for user data

7.6 Hitag 2 (256 bit, 32 Bytes)

Memory blocks (pages) of 32 bit/4 Bytes.

Block #	Hex Address	Access	Description
1	00	Read-only	UID
2	01	Read/Write	Passwort RWD, standard 4D494B52h
3	02	No Access	—
4	03	Read/Write	Configuration word, password-protected, standard PW 0000 0000 h
5	04	Read/Write	Memory for user data / 64 bit for Read-only-Emulation
6	05	Read/Write	Memory for user data / 64 bit for Read-only-Emulation
7	06	Read/Write	Memory for user data
8	07	Read/Write	Memory for user data

7.7 EM4450/4550 (1 kbit)

Memory blocks (pages) of 32 bit/4 Bytes.

Block #	Hex Address	Access	Description
1	00	Read-only	Password, standard 00000000h
2	01	Read-only	Security word
3	02	Read-only	Control word
4	03	Read/Write	Memory for user data
…	…	…	Memory for user data
31	1F	Read/Write	Memory for user data
32	20	Read-only	Device Serial Number (UID)
33	21	Read-only	Device Identification