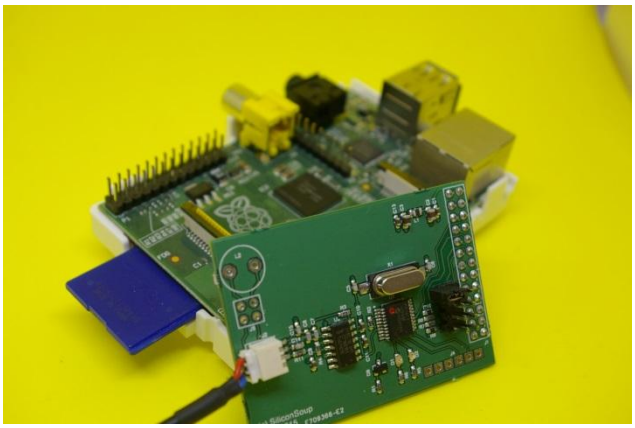
OVERVIEW



The Pi RFID Reader is a complete 125kHz reader solution for the Raspberry Pi. It supports Hitag 1, Hitag S256/S2048 (RTF / Plain Memory mode), Hitag 2 (Password mode), EM400X/4102 and MCRF200/123 passive RFID transponder types. The solution only needs a 770 µH antenna coil connected and 5v DC supply to be a fully featured read/write system.

The Reader offers one of the best OOB (out of box) experiences for Pi based RFID readers. By using the UART of the Pi for communication and the built in intelligence of the Reader the user is able to operate the reader without the need for libraries to be downloaded and compiled onto the Pi. The reader is intelligent and performs reading and writing of tags independently of the Pi. All of the tag read/write data is available to the Raspberry Pi.

LEDs indicate the Reader activity without any intervention from the Raspberry Pi. The red LED is normally ON until a valid card or tag is brought into the RF field of the antenna. If the tag is accepted as valid then the green LED is turned ON (Red OFF). The reader can also check for a broken or shorted antenna and can even detect a badly tuned antenna, these problems are indicated by the red LED “flashing” continuously until the fault has been rectified.

The Reader may be customised by the host and configurations changed. The READER TYPE command code (ASCII "v", 0x76) plus a parameter byte can be used to select one of the Hitag1/S, Hitag 2 or EM400X transponder modes, a parameter in the EEPROM map further selects between EM400X and MC200/123 types.

The Reader adds very little to the power budget of the Raspberry Pi, consuming about 1mA.

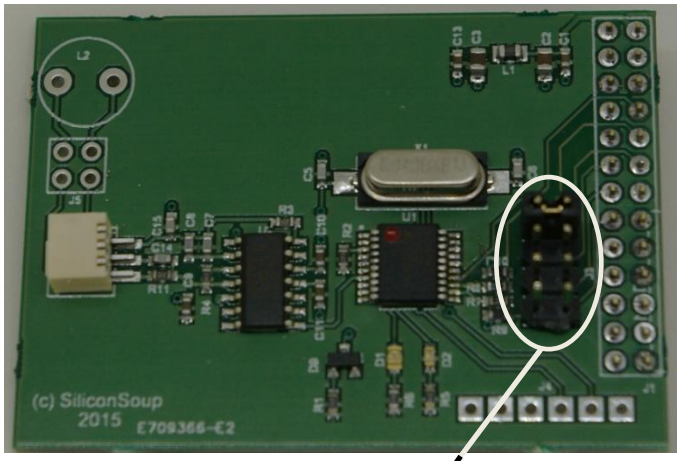
The Reader is a proximity system and a Read/Write range of up to 15cm (dependent on antenna size) can be achieved with the same level of reliable communication and EMC resilience. The unique AST (Adaptive Sampling) feature allows the Reader to continually adjust and re-tune the sampling to allow for inductive changes in the RF field, an essential feature for real-world reliability and robust operation. The Reader automatically scans for tags and does not need a host system connected to identify a tag in the field.

The communication protocol with the tags can achieve up to 4k bits/second of data transfer and the total time, for example, to read a Hitag 1/S or Hitag 2 four-byte page takes less than 100ms.

READER FEATURES

An onboard antenna could be connected to L2

Antenna Connector



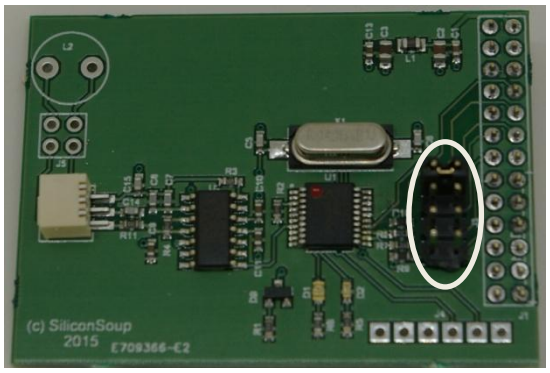
Connector for Raspberry Pi

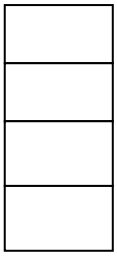
Jumpers – See section on Configuration

CONTENTS

CONFIGURATION

The Reader has some options to enable the user to select which GPIO of the Raspberry Pi is used.





Jumper 1. GPIO18
Jumper 2, GPIO17
Jumper 3, GPIO21
Jumper 4, GPIO22

Only one jumper should be connected at any time. For example, connecting the jumper across the jumper 1 pins enables the Pi to select the Reader using GPIO18.

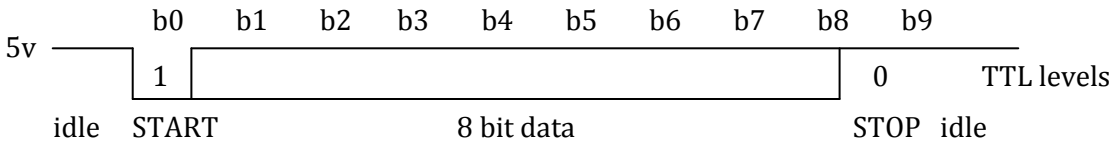
COMMUNICATION INTERFACE

The Raspberry Pi communicates with the Reader using its UART. Data is sent to the Reader using the Tx pin and data from the Reader to the Pi uses the Rx line.

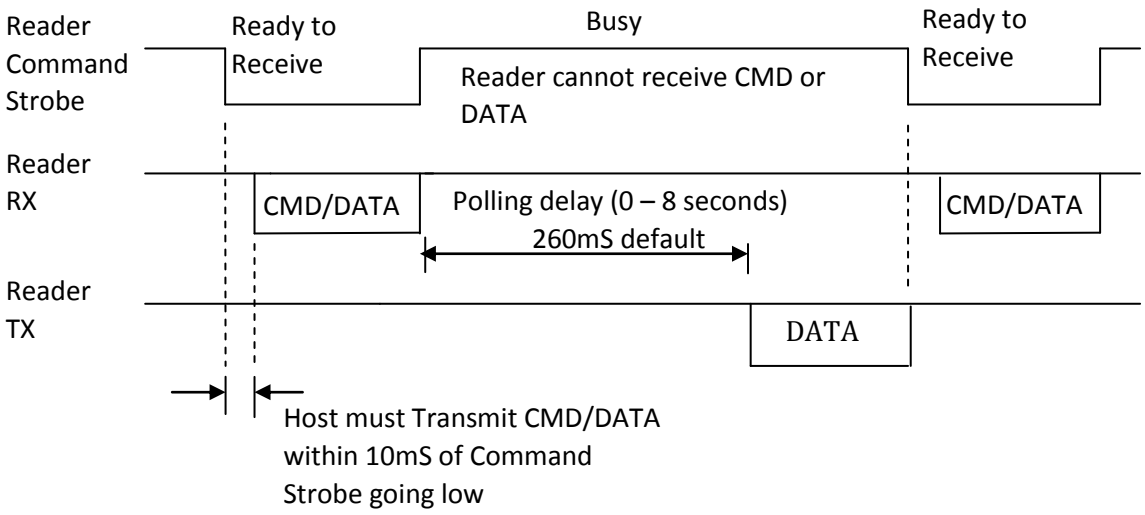
When the Reader is ready to accept a command from the Pi it sets the Command Strobe low. The jumper connects the Command Strobe to one of the Pi GPIO ports (see the Configuration section). Only one command with associated parameters is handled each time the Command Strobe goes low.

The UART must be set for 9600 baud, 8-bits, 1-stop, no parity (104uS per bit).

The Reader uses the Command Strobe to signal to the Pi when it is ready for communications and when to inhibit communications from the host (when the Reader is fully occupied with RF communication).



The serial communication system and protocol allows for a 10ms ‘window’ every Tag polling cycle indicated by the Command Strobe line being low. During this ‘window’ the host must assert the first start bit and start transmitting data. The Command Strobe goes high again 10ms after the last stop bit is received. NOTE that only one command sequence is handled at a time.



NOTE that the (programmable) polling delay period is skipped if the EEPROM parameter is zero or if there are commands to be processed.

SUMMARY OF COMMANDS AND RESPONSES

Command and associated parameter bytes are sent to the Reader immediately Command Strobe goes LOW. For example to READ PAGE 0, when Command Strobe signal goes low, immediately send 0x52 0x00 as hex bytes.

The reader replies with C0 hex status/acknowledge byte if no tag present or D6 hex status/acknowledge byte (indicating tag present and received OK) followed b 4-bytes of data from page read.

Command (all operating modes)	Operation and Typical Response (with no errors detected)
CARD STATUS, ASCII “S”, 0x53	Returns status/acknowledge byte 0xC0 if no card, 0xD6 if card present
VERSION MESSAGE, ASCII “z”, 0x7A	Returns “firmware version message” with 0x00 at end
READER MODE, ASCII “v”, 0x76 Send 0x76 0xMM	Selects Reader operating mode, MM = 01 (H2), 02 (H1/S – factory default), 03 (EM/MC200 mode), 0xC0 reply
PROGRAM EEPROM, ASCII “P”, 0x50 Send 0x50 0xLL 0xPP	Stores 0xPP value at EEPROM location 0xLL and internally verifies, 0xC0 reply
FACTORY RESET, ASCII “F”, 0x46 Send 0x46 0x55 0xAA	Restores Factory default settings in EEPROM and resets. No reply

Command (HITAG1/S mode)	
WRITE H1/S PAGE, ASCII "W", 0x57 Send 0x57 0xNN 0xDD 0xDD 0xDD 0xDD	Write to H1/S card PAGE NN 4-bytes of data 0xDD – 0xDD Returns status/acknowledge byte 0xC0 if no card or 0xD6 if successful
WRITE H1/S BLOCK, ASCII "w", 0x77 Send 0x77 0xNN 0xDD – 0xDD BLOCK = 4 x PAGEs (up to 16-bytes)	Write to H1/S card BLOCK (PAGE NN+0, +1, +2, +3) up to 16-bytes of data 0xDD – 0xDD Perform PAGE/4 => if remainder (mod) = 0 then full block (16 bytes) if remainder = 1 then 12 bytes sent if remainder = 2 then 8 bytes sent if remainder = 3 then 4 bytes (1 x PAGE) sent Returns 0xC0 if no card or 0xD6 if successful
READ H1/S PAGE, ASCII "R", 0x52 Send 0x52 0xNN	Read H1/S PAGE NN (0-63) Returns status/acknowledge byte 0xC0 if no card or 0xD6 0xDD 0xDD 0xDD 0xDD Where 0xDD – 0xDD is 4-bytes of data read
READ H1/S BLOCK, ASCII "r, 0x72 Send 0x72 0xNN BLOCK = 4 x PAGEs (up to 16-bytes)	Read H1/S card BLOCK (PAGE NN+0, +1, +2, +3) up to 16-bytes of data. Perform PAGE/4 => if remainder (mod) = 0 then full block read (16 bytes) if remainder = 1 then 12 bytes read if remainder = 2 then 8 bytes read if remainder = 3 then 4 bytes (1 x PAGE) read Returns 0xC0 if no card or 0xD6 0xDD – 0xDD (where 0xDD – 0xDD is up to 16-bytes of data) if successful
Command (HITAG2 mode)	
WRITE H2 PAGE, ASCII "W", 0x57 Send 0x57 0xNN 0xDD 0xDD 0xDD 0xDD	Write to H2 card PAGE NN 4-bytes of data 0xDD – 0xDD Returns status/acknowledge byte 0xC0 if no card or 0xD6 if successful
READ H2 PAGE, ASCII "R", 0x52 Send 0x52 0xNN	Read H2 PAGE NN (0-7) Returns status/acknowledge byte 0xC0 if no card or 0xD6 0xDD 0xDD 0xDD 0xDD Where 0xDD – 0xDD is 4-bytes of data read
Command (EM400x / EM4102 mode)	
READ EM4102 tag, ASCII "R", 0x52 Send 0x52 0xNN	Read EM4102 NN (dummy page byte 0x00) Returns status/acknowledge byte 0xC0 if no card or 0xD6 0xDD 0xDD 0xDD 0xDD 0xDD Where 0xDD – 0xDD is 5-bytes of data read

Command (MCRF200 mode)	
READ MCRF200 tag, ASCII "R", 0x52 Send 0x52 0xNN	Read MCRF200 NN (dummy page byte 0x00) Returns status/acknowledge byte 0xC0 if no card or 0xD6 0xDD -0xDD Where 0xDD – 0xDD is 16-bytes of data read

SUPPORTED TRANSPONDER TYPES

The Reader is designed to communicate with the following 125kHz passive RF transponder types:-

1) Hitag 1 read/write transponders configured in R/W Public mode. Setting the HT1 to any other configuration will render them inoperable with this system. Note: Only the HT1 ICS30 02x Hitag silicon is fully supported for WRITE/ READ operations. The earlier HT1 ICS30 01x silicon (made obsolete by NXP) is only partially supported.
2) Hitag S256, S2048 read/write transponders configured in PLAIN MEMORY mode (NXP factory default). Reader support is default RTF (Reader transmits first) mode.
3) Hitag 2 read/write transponders configured in PASSWORD mode. Setting the HT2 transponder to any other configuration will render them inoperable with this system.
4) EM Marin EM4001/H4001 type transponders including H4003, H4102 and compatible read-only tags with the correct header, data and parity bit structure.
5) Microchip Technology MCRF 200-I/123 RF transponders that use direct ASK modulation, Manchester coding and with a data rate of RF/64. The MCRF200 transponder is expected to have the 0x802A header sequence at the start of the memory array.

The transponder identification codes described in this text are regarded as the first four bytes (serial number or page 0) of the H1 and H2 memory array or bytes 1 to 4 (least significant four bytes) of the EM400X and MCRF200 memory arrays (ignoring most significant byte 0).

RASPBERRY PI DRIVER SOFTWARE

Example software for the Raspberry Pi is available on www.Bostintechnology.com.

TYPICAL HOST COMPUTER "PSEUDO" DRIVER CODE

```
if (Green LED ON (pin 2 = 0))          // Optional check for valid tag in field
{
   if (Command Strobe = 0)             // Wait for Command Strobe = 0 (Reader ready to receive command / data)
  {
          // Command Strobe times out after 10ms so command and all parameters must be sent with no-
          // gaps otherwise Command Strobe times out and goes HIGH.
          // For example, send READ PAGE 1 (0x52 0x01)
```

```
        SEND_CMD( );   // Sent command + parameters to MTRW

        // Reader sets Command Strobe = 1 after last parameter received. Reader enters low-
        // power state during (programmable) polling delay then sends reply.

        GET_REPLY( );              // Get Acknowledge byte + data
        // Response to READ command is 0xC0 (no tag) or 0xD6 + four bytes of DATA.
  }
}
```

COMMAND PROTOCOL

The commands are described fully in the following pages. The STATUS, MESSAGE and PROGRAM EEPROM commands are common to all the Reader modes, the structure and reply from commands such as READ PAGE can be different depending on which Reader mode is selected. Generally, command codes (plus optional data bytes) are transmitted to the Reader which replies with a Status/Acknowledge byte (and data bytes if appropriate). The Acknowledge code should be read back by the host and decoded to confirm that the command was received and handled correctly. The serial bit protocol is 9600 baud, 8 bits, 1 stop, no parity (lsb transmitted first).

The status flags returned in the Acknowledge byte are as follows:

```
 b7  b6  b5  b4  b3  b2  b1  b0
 1   1   1   1   1   1   1   1
         |   |   |   |   |   EEPROM error (Internal EEPROM write error)
         |   |   |   |   Tag OK (Tag identity code matched to list)
         |   |   |   Rx OK  (Tag  communication and acknowledgement OK)
         |   |   RS232  error (Host serial communication error)
         |   RELAY Enabled flag
    HTRC (or Antenna fault) error flag
```

Typical status/acknowledge byte response:
0xC0 - no tag
0xD6 - tag present and no errors.

Note that bits 6 and 7 are fixed 1's so that an acknowledge code of C0 (Hex) would indicate NO valid transponder in the RF field, whereas an acknowledge byte of D6 (Hex) would indicate a correctly matched transponder detected in the field (and no errors).
Note also that only the relevant flags are set after each command as indicated in the protocol documents.
NOTE:

1) The serial communication uses hardware handshaking to inhibit the host from sending the Reader commands while RF tag communication is in progress.

2) Following the Read Tag command, if an error flag has been set in the Acknowledge code then there will be NO data.
3) The serial communication system and protocol allows for a 10ms 'window' every Tag polling cycle indicated by the Command Strobe line being low. During this 'window' the host must assert the first start bit and start transmitting data. The Command Strobe goes high again 10ms after the last stop bit is received.
4) NOTE that only one command sequence is handled at a time.

TAG STATUS

Command to return Tag status. The acknowledge byte flags indicate general Tag status.

	B7						B0	
Command:	0	1	0	1	0	0	1	1	(ASCII "S", 0x53)
Acknowledge:	1	1	F	F	F	F	F	X	(F = Status flags)

MESSAGE

Command to return product and firmware identifier string to host.

	B7						B0	
Command:	0	1	1	1	1	0	1	0	(ASCII "z", 0x7A)

Reply: "b IDE MTRW H1 (firmware filename V1.xx) DD/MM/YY) Copyright message" 0x00

Returned string identifies author, product descriptor, project name, firmware version no. and date of last software change. Note that the string is always NULL terminated. The string begins with a unique lower case character that can be used to identify a particular version of Reader.

READER MODE

Command to allow selection of particular "Reader Mode". This command has the same function as writing to parameter byte 17 (0x11) of the internal EEPROM using Program EEPROM command. The Acknowledge byte reply confirms if parameter has been stored correctly.

	B7							B0	
Command:	0	1	1	1	0	1	1	0	(ASCII "v", 0x76)
Argument1:	X	X	X	X	X	X	N	N	(NN bits = Reader Type selection parameter) 01 = Hitag 2 (0x01) 10 = Hitag 1/S (0x02 – factory default) 11 = EM400X/MC200 (0x03) (00 parameter also selects Hitag 1 version)
Acknowledge:	1	1	X	F	X	X	X	F	(F = Status flags, X = "don't care" bits)

The "Reader Mode" command has been added to the standard command set in order to allow selection of the H1/S, H2 or EM400X Reader modes. This command automatically stores the "Reader Mode" parameter in the Reader internal EEPROM (parameter byte 17) to allow the required Reader Type selection from power-up. The standard PROGRAM EEPROM command can also be used to store the parameter byte directly to location 17 to achieve the same result.
When EM400X type is selected, MCRF200/123 transponder type can be further selected as a subset of the main EM400X option. This achieved by storing 00 as the "EM400X/MC200" selection parameter (byte 16) in the internal EEPROM (using Program EEPROM command). Storing 01 as the selection parameter selects main EM400X type (factory default set to 01, EM400X mode).
The selected Reader Type can be verified by sending the MESSAGE command (0x7A = ASCII "z").
The message string returned has a unique ASCII character as the start of the string ("a", "b" or "c") and this can be used to confirm Reader mode currently selected.

FOR EXAMPLE:-

H1 type selected, MESSAGE command reply =
"**b** IDE MTRW H1 (MTRW_LP V1.xx) DD/MM/YY) Copyright IB Technology Ltd" 0x00

H2 type selected, MESSAGE command reply =
"**a** IDE MTRW H2 (MTRW_LP V1.xx) DD/MM/YY) Copyright IB Technology Ltd" 0x00

EM400X/MC200 type selected, MESSAGE command reply =
"**c** IDE MTRW EM400X/MC200 (MTRW_LP V1.xx) DD/MM/YY) Copyright IB Technology Ltd" 0x00

PROGRAM EEPROM

The Reader has internal EEPROM for storing system parameters such as passwords and authorised identity codes. This command sequence allows individual bytes of the EEPROM to be programmed with new data. Note that due to the fundamental nature of these system parameters, incorrect data may render the system temporarily inoperable.

	B7						B0	
Command:	0	1	0	1	0	0	0	0	(ASCII "P", 0x50)
Argument1:	N	N	N	N	N	N	N	N	(N = EEPROM memory location 0 - 255)
Argument2:	D	D	D	D	D	D	D	D	(D = data to write to EEPROM)
Acknowledge:	1	1	X	F	X	X	X	F	(F = Status flags)

INTERNAL EEPROM MEMORY MAP

Polling delay parameter values (EEPROM location 0):

Parameter 0 value	Polling Delay SLEEP Period
0x00	0 mS
0x10	8 mS
0x20	16 mS
0x30	32 mS
0x40	65 mS
0x50	132 mS
0x60	**262 mS**
0x70	524 mS
0x80	1 second
0x90	2 seconds
0xA0	4 seconds
0xB0	8 seconds

Polling delay and SLEEP skipped

Polling delay can be set from 0 to 8 seconds. Note that setting Polling delay = 0x00 skips the delay so polling is as fast as possible. Polling delay is also skipped when there are host commands to be processed.

Byte 0: Polling Delay period (Default = 0x60 = approx 260mS)
Byte 1: RF ON/OFF lock byte (0x55 = RF ON, anything else = OFF, default set to 0x55)
Byte 2: Reserved (internal checksum value) – RESERVED - do not use
Byte 3: H1 Encryption ON/OFF control byte (0x00 = OFF)

Byte 4:) H1 32 bit Encryption Seed (M.S byte)
Byte 5:)
Byte 6:)
Byte 7:) (L.S byte)

Byte 8:	H2 PASSWORD_RWD (32 bit password sent to HT2) – default “M”
Byte 9:	H2 PASSWORD_RWD “I ”
Byte 10:	H2 PASSWORD_RWD “K”
Byte 11:	H2 PASSWORD_RWD “R”
Byte 12:	Reserved (not used)
Byte 13:	H2 PASSWORD_TAG (24 but reply from HT2) - default 0xAA
Byte 14:	H2 PASSWORD_TAG "H"
Byte 15:	H2 PASSWORD_TAG "T"
Byte 16:	EM400X Option Byte, 0x00 = MC200, 0x01 = EM400x (default)
Byte 17:	Reader Type (0x02 = H1 default)
Byte 18:	Reserved (not used)
Byte 19:	Reserved (not used)

FACTORY RESET

Command to restore Factory default EEPROM values and perform hardware Reset operation. The 0x55 0xAA parameters protect against accidental operation.
After Reset, the Green LED flashes five times indicating the successful loading of the Factory default values.

	B7							B0	
Command:	0	1	0	0	0	1	1	0	(Ascii “F”, 0x46)
Argument1:	0	1	0	1	0	1	0	1	0x55
Argument1:	1	0	1	0	1	0	1	0	0xAA

Reset occurs after the command is processed so there is no Acknowledge byte reply.

READER HITAG 1/S COMMAND PROTOCOL

The reader H1/S Reader mode is a complete read / write and tag acceptance solution for Hitag 1, Hitag S256 and Hitag S2048 RFID transponders (in “NXP default” RTF/Reader Transmits First, Plain Memory mode).

WRITE H1/S TAG PAGE

Command to write 4 bytes of data to HT1 32 bit page. If the write was unsuccessful (invalid tag or out of field) then Status flags in acknowledge byte indicate error.

	B7							B0	
Command:	0	1	0	1	0	1	1	1	(ASCII “W”, 0x57)

Argument1:	x x N N N N N N	(N = HT1 page address 0-63)
Argument2:	D D D D D D D D	(D = msb data to write to HT1)
Argument3:	D D D D D D D D	
Argument4:	D D D D D D D D	
Argument5:	D D D D D D D D	(D = lsb data to write to HT1)
Acknowledge:	1 1 F F F F F X	(F = Status flags)

WRITE H1/S TAG BLOCK

Command to write up to 16 bytes of data to HT1 memory. A Block is made up of four pages (each page being 4 bytes of data). If the specified page lies on the block boundary then all 16 bytes (4 pages) can be written. If the specified page is on the block boundary + 1 then 12 bytes (3 pages) can be written.
In this way 16, 12, 8 or 4 bytes of data can be stored on the tag depending on the page number and its position within the block. If the write was unsuccessful (invalid tag or out of field) then Status flags in acknowledge byte indicate error.

	B7 B0	
Command:	0 1 1 1 0 1 1 1	(ASCII “w”, 0x77)
Argument1:	x x N N N N N N	(N = HT1 page address 0-63)
Argument2:	D D D D D D D D	(D = msb data to write to HT1)
Argument3:	D D D D D D D D	(PAGE N DATA)
Argument4:	D D D D D D D D	
Argument5:	D D D D D D D D	(D = lsb data to write to HT1)

|
| Up to 16 bytes can be specified depending on page address N
| ie. Perform PAGE/4 => if remainder (mod) = 0 then full block (16 bytes)
| if remainder = 1 then 12 bytes sent
| if remainder = 2 then 8 bytes sent
| if remainder = 3 then 4 bytes sent
V

Argument14:	D D D D D D D D	(D = msb data to write to HT1)
Argument15:	D D D D D D D D	(PAGE N+3 DATA)
Argument16:	D D D D D D D D	
Argument17:	D D D D D D D D	(D = lsb data to write to HT1)
Acknowledge:	1 1 F F F F F X	(F = Status flags)

READ H1/S TAG PAGE

Command to read 4 bytes of data from HT1 32 bit page. If the read was successful, indicated by acknowledge status flags then four bytes of tag data follow.

	B7						B0	
Command:	0	1	0	1	0	0	1	0	(ASCII "R", 0x52)
Argument1:	x	x	N	N	N	N	N	N	(N = HT1 page address 0-63)
Acknowledge:	1	1	F	F	F	F	F	X	(F = Status flags)
Data only follows if read was successful									
Reply1:	D	D	D	D	D	D	D	D	(D = msb data read from HT1)
Reply2:	D	D	D	D	D	D	D	D	
Reply3:	D	D	D	D	D	D	D	D	
Reply4:	D	D	D	D	D	D	D	D	(D = lsb data read from HT1)

READ H1/S TAG BLOCK

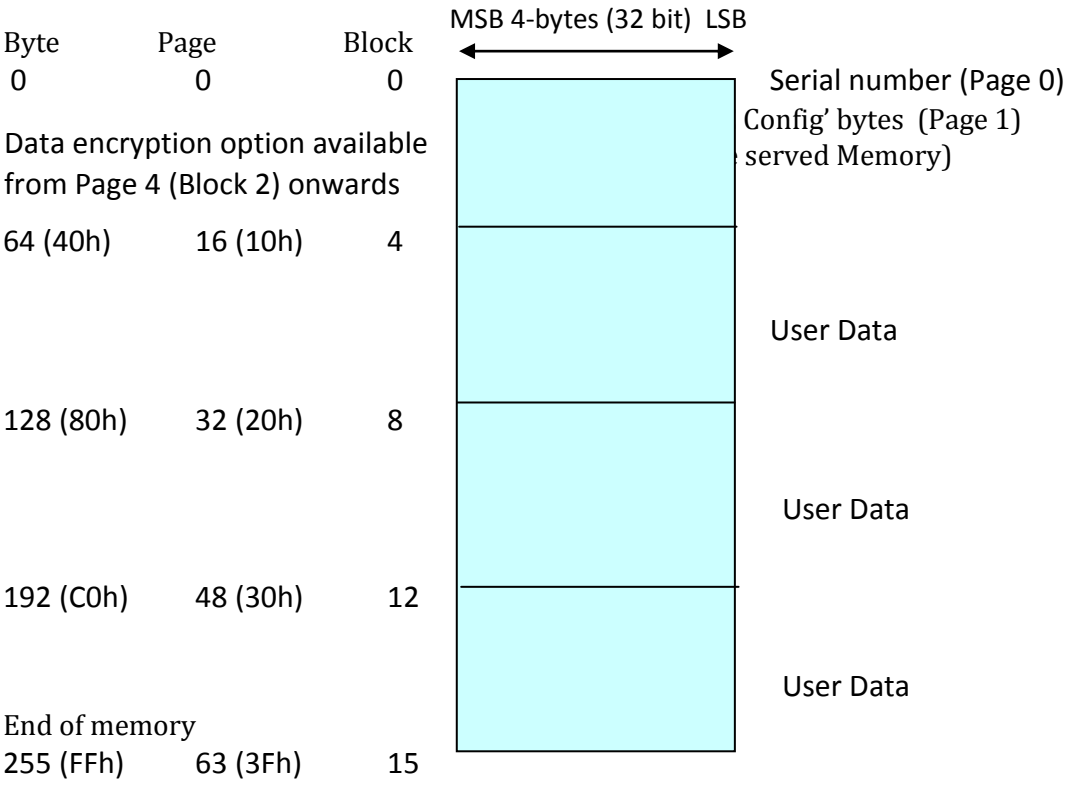
Command to read up to 16 bytes of data from HT1 memory. A Block is made up of four pages (each page being 4 bytes of data). If the specified page lies on the block boundary then all 16 bytes (4 pages) can be read. If the specified page is on the block boundary + 1 then 12 bytes (3 pages) can be read. In this way 16, 12, 8 or 4 bytes of data can be retrieved from the tag depending on the page number specified and its position within the block. If the read was successful, indicated by acknowledge status flags then up to 16 bytes of tag data follow.

	B7						B0	
Command:	0	1	1	1	0	0	1	0	(ASCII "r", 0x72)
Argument1:	x	x	N	N	N	N	N	N	(N = HT1 page address 0-63)
Acknowledge:	1	1	F	F	F	F	F	X	(F = Status flags)
+ up to 16 bytes									
Data only follows if read was successful									
Reply1:	D	D	D	D	D	D	D	D	(D = msb data read from HT1)
Reply2:	D	D	D	D	D	D	D	D	(PAGE N DATA)
Reply3:	D	D	D	D	D	D	D	D	
Reply4:	D	D	D	D	D	D	D	D	(D = lsb data read from HT1)

|	
|	Up to 16 bytes can be specified depending on page address N
|	ie. Perform PAGE/4 => if remainder (mod) = 0 then full block (16 bytes)
|	if remainder = 1 then 12 bytes read
|	if remainder = 2 then 8 bytes read
|	if remainder = 3 then 4 bytes read
V	

Reply13:	D D D D D D D D	(D = msb data read from HT1)
Reply14:	D D D D D D D D	(PAGE N+3 DATA)
Reply15:	D D D D D D D D	
Reply16:	D D D D D D D D	(D = lsb data read from HT1)

HITAG 1 MEMORY MAP

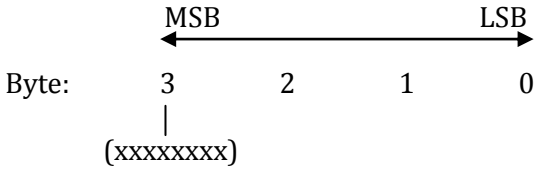


Hitag 1 transponders have Pages 16 to 63 available for user data storage (192 bytes). It is advised not to use the memory locations below page 16 because these are used for configuration bytes and a "Reserved" memory area.

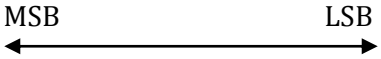
Hitag S transponders configured in PLAIN MEMORY mode have a similar memory map to Hitag 1 except they have available "user data " memory from Page 2 onwards. Hitag S256 transponders therefore have Page 2 – 7 (24 bytes) for user data and Hitag S2048 types have Page 2 - 63 (248 bytes) for user data.

HITAG 1 SERIAL NUMBER AND CONFIGURATION BYTES

Page 0 (Serial Number):



Page 1 (Configuration Bytes):



Byte: 3 2 1 0

Read/Write Read/Write CON1 CON0

The Hitag 1 configuration bytes control whether the memory blocks are read/write or locked for read only access. Note that bytes 2 and 3 of the configuration page are not used and are currently available for general read/write use.

CON 0 (Page 1, byte 0)

```
b7  b6  b5  b4  b3  b2  b1  b0
 1   1   |   |   |   |   |   0 = Block 7 read only
         |   |   |   |   |   1 = Block 7 read/write
         |   |   |   |   0 = Block 6 read only
         |   |   |   |   1 = Block 6 read/write
         |   |   |   0 = Block 5 read only
         |   |   |   1 = Block 5 read/write
         |   |   0 = Block 4 readonly
         |   |   1 = Block 4 read/write
         |   0 = Block 3 read only
         |   1 = Block 3 read/write
         0 = Block 2 read only
         1 = Block 2 read/write
```

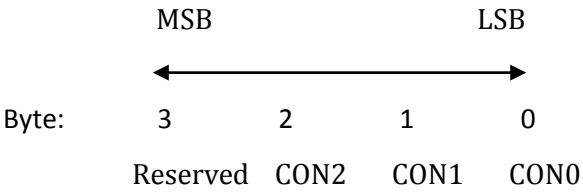
CON 1 (Page 1, byte 1)

```
b7  b6  b5  b4  b3  b2  b1  b0
 |   |   |   |   |   |   |   1
 |   |   |   |   |   |   |
 |   |   |   |   |   |   Reserved
 |   |   |   |   |   |
 |   |   |   |   |   Reserved
 |   |   |   |   |
 |   |   |   |   Reserved
 |   |   |   |
 |   |   |   0 = Configuration (Page 1) read only
 |   |   |   1 = Configuration (Page 1) read/write
 |   |   Reserved
 |   |
 |   Reserved
 |
Reserved
```

Note that these configuration bits are OTP. Once they are set to read-only the Hitag 1 transponder is hardware protected and they can never be changed.

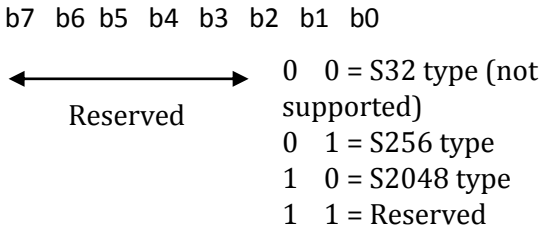
Note that the "Reserved" bits of Configuration Byte 1 must not be altered. Page 1 must be read first and the bits that can be changed masked on/off before writing back.

HITAG S CONFIGURATION BYTES

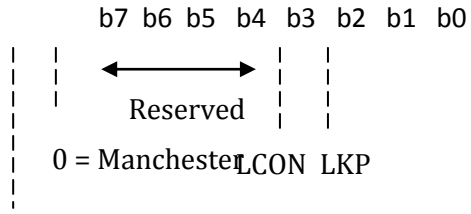


The Hitag S configuration bytes indicate the type of HS transponder and the mode of operation. Please note that the Reader H1/S mode only supports RTF (Reader Transmits First) and Plain Memory mode (default mode as set by NXP/Philips). Configuration bytes also control whether the memory blocks are read/write or locked for read only access.

CON 0 (Read-only – Memory Type information)



CON 1 (Mode and Lock bits)

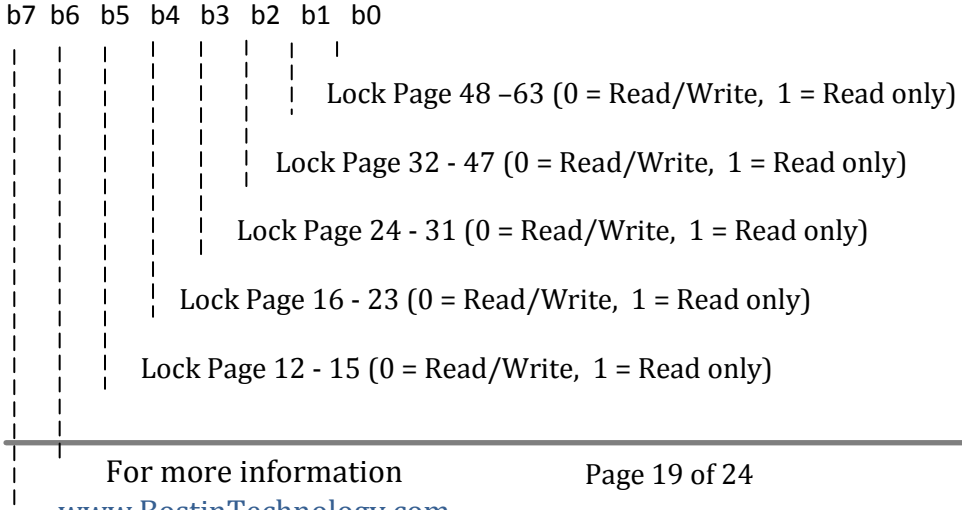


0 = Plain Memory mode
1 = Authentication mode not supported

LCON bit
(CON1 and CON2 access control):
0 = Read/Write
1 = CON1 read only, CON2 OTP

LKP bit
(Page 2 and Page 3 access control)
0 = Read/Write
1 = Read only.

CON 2 (Memory Lock bits)



Lock Page 8 - 11 (0 = Read/Write, 1 = Read only)

Lock Page 6 - 7 (0 = Read/Write, 1 = Read only)

Lock Page 4 - 5 (0 = Read/Write, 1 = Read only)

Note that CON2 (Memory Lock bits) are OTP (One-Time-Programmable) if LCON = 1
Note also that the "Reserved" bits must not be altered. Page 1 must be read first and the bits that can be changed masked on/off before writing back.

READER HITAG 2 COMMAND PROTOCOL

The Reader H2 Reader mode a complete read / write and tag acceptance solution for Hitag 2 RFID transponders (in Password mode).

WRITE H2 TAG PAGE

Command to write 4 bytes of data to HT2 32 bit page. If the write was unsuccessful (invalid tag or out of field) then Status flags in acknowledge byte indicate error.

	B7							B0	
Command:	0	1	0	1	0	1	1	1	(ASCII "W", 0x57)
Argument1:	x	x	x	x	x	N	N	N	(N = HT2 page address 0-7)
Argument2:	D	D	D	D	D	D	D	D	(D = msb data to write to HT2)
Argument3:	D	D	D	D	D	D	D	D	
Argument4:	D	D	D	D	D	D	D	D	
Argument5:	D	D	D	D	D	D	D	D	(D = lsb data to write to HT2)
Acknowledge:	1	1	F	F	F	F	F	X	(F = Status flags)

Note that PASSWORD exchange occurs for WRITE command.
If no tag present then acknowledge / status byte reply is 0xC0
If tag present but RWD PASSWORD check fails then acknowledge byte reply is 0xC0.
If tag present but TAG PASSWORD check fails then acknowledge byte reply is 0xC4.
If tag present and both PASSWORDS match then acknowledge reply is 0xD6.

READ H2 TAG PAGE

Command to read 4 bytes of data from HT2 32 bit page. If the read was successful, indicated by acknowledge status flags then four bytes of tag data follow.

	B7							B0	
Command:	0	1	0	1	0	0	1	0	(ASCII "R", 0x52)
Argument1:	x	x	x	x	x	N	N	N	(N = HT2 page address 0-7)

Acknowledge: 1 1 F F F F F X (F = Status flags)

Data only follows if read was successful

Reply1: D D D D D D D D (D = msb data read from HT2)
Reply2: D D D D D D D D
Reply3: D D D D D D D D
Reply4: D D D D D D D D (D = lsb data read from HT2)

Note that PASSWORD exchange occurs for READ command.
If no tag present then acknowledge / status byte reply is 0xC0
If tag present but RWD PASSWORD check fails then acknowledge byte reply is 0xC0.
If tag present but TAG PASSWORD check fails then acknowledge byte reply is 0xC4.
If tag present and both PASSWORDS match then acknowledge reply is 0xD6 followed by 4-bytes of data.

HITAG 2 MEMORY MAP (PASSWORD MODE)

The memory of the Hitag 2 transponder consists of 256 bits of low power EEPROM memory which is organised into 8 pages of 32 bits (4 bytes) each.

Page No.	Content (32 bit words/ 4 bytes)
0	Serial number
1	PASSWORD RWD (DEFAULT = "MIKR" = 4D 49 4B 52 HEX)
2	Reserved
3	**8 bit Configuration, 24 bit Password TAG (Default = 06 AA 48 54 hex)**
4	Read/Write page
5	Read/Write page
6	Read/Write page
7	Read/Write page

HITAG 2 CONFIGURATION BYTE

The 8 bit configuration byte located at the start of page 3 defines the basic mode of the Hitag 2 transponder and whether certain parts of its memory are locked or open for Read/Write operations. Note that the Reader in H2 Reader mode only supports PASSWORD operating mode and can communicate with Hitag 2 tags with the **configuration byte = 0x06** (or 0x46 with configuration and TAG Password locked).

CONFIGURATION OR PASSWORDS MUST NOT BE CHANGED UNLESS THE OPERATION OF THE HITAG 2 TRANSPONDER IS UNDERSTOOD.

Configuration Byte (Page 3, byte 0)

b7	b 6	b5	b4	b3	b2	b1	b0
|	|	|	|	**0**	**1**	**1**	**0**

| | | | 0 = Page 6 and 7 read/write
| | | | 1 = Page 6 and 7 read only
| | | |
| | | 0 = Page 4 and 5 read/write
| | | 1 = Page 4 and 5 read only
| | |
| | 0 = Page 3 read/write
| | 1 = Page 3 read only, Configuration and TAG Password **FIXED**, THIS BIT IS OTP
| |
0 = Page 1 an 2 read/write
1 = Page 1 no read/no write, Page 2 (RWD Password) read only, THIS BIT IS OTP

READER EM400X / EM4102 COMMAND PROTOCOL

The MTRW H400X Reader mode is a complete reader and tag acceptance solution for EM Marin (EM)H4001/H4102 and compatible RFID transponders.

READ EM/H400X TAG

Command to read 5 bytes of data from H400x (40 bit) memory array. If the read was successful, indicated by acknowledge status flags then five bytes of tag data follow.

	B7 B0	
Command:	0 1 0 1 0 0 1 0	(ASCII “R”, 0x52)
Argument1:	x x x x x x x x	(Dummy Page number e.g 00)
Acknowledge:	1 1 F F F F F X	(F = Status flags)
Data only follows if read was successful		
Reply1:	D D D D D D D D	(D = msb data read from H400x)
Reply2:	D D D D D D D D	
Reply3:	D D D D D D D D	
Reply4:	D D D D D D D D	
Reply5:	D D D D D D D D	(D = lsb data read from H400x)

Note that for the Read Tag command, if an error flag has been set in the Acknowledge code then there will be NO following data.

MTRW MC200 COMMAND PROTOCOL

The MTRW MC200 Reader mode is a complete reader and tag acceptance solution for Microchip Technology MCRF 200-I/123 RFID read-only transponders (configured as RF/64 bit rate, direct ASK, Manchester coded with 0x802A header bytes)

READ MC200 TAG

Command to read 16 bytes of data from MCRF200 (128 bit) memory array. If the read was successful, indicated by acknowledge status flags then 16 bytes of tag data follow.

```
                B7                  B0
Command:     0  1  0  1  0  0  1  0        (ASCII "R", 0x52)
Argument1:   x  x  x  x  x  x  x  x        (Dummy Page number e.g 00)

Acknowledge:  1  1  F  F  F  F  F  X        (F = Status flags)

Data only follows if read was successful
Reply1:              D  D  D  D  D  D  D  D     (D = msb data read from MCRF200)
Reply2:              D  D  D  D  D  D  D  D
Reply3:              D  D  D  D  D  D  D  D
  |
  v
Reply15:     D  D  D  D  D  D  D  D
Reply16:     D  D  D  D  D  D  D  D     (D = lsb data read from MCRF200)
```

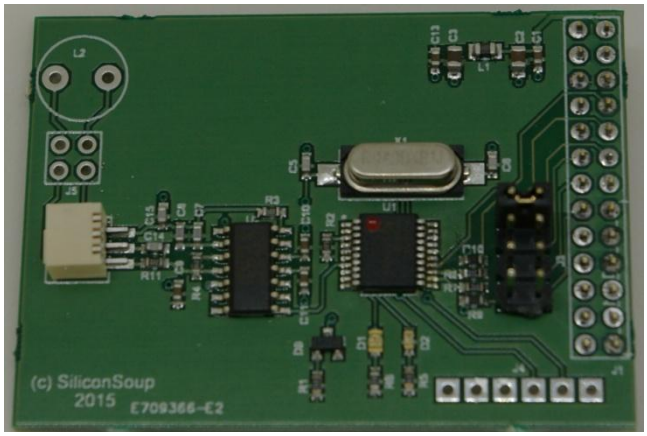
Note that for the Read Tag command, if an error flag has been set in the Acknowledge code then there will be NO following data.

READER SPECIFICATIONS

Parameter	Typical Value
Supply Voltage (performance optimised for 5 volt operation)	4 – 6 volts DC (operation from 4 x alkaline cells)
Operating temperature	-40 deg C to + 85 deg C
AVERAGE current consumption.	**<2mA**
Active period for RF AND host communication (each polling cycle).	Up to 40 mS
Peak antenna voltage (optimum tuning)	180 volts peak-to-peak
Peak antenna current (optimum tuning) for short period each polling cycle (up to 10 mS burst)	150 mA
Polling Delay (SLEEP / Power-down mode)	0 to 8 seconds
Maximum data rate (between card and Reader)	4k baud
Range (dependent on antenna dimensions and tuning)	Up to 150mm
Serial Interface	UART
Serial Communication Parameters	9600 baud, 8 data bits, no parity, 1 stop bit protocol with Command Strobe handshake

Basic electrical specification with LEDs pins and auxiliary outputs NOT connected.
Note that the Reader version is designed for optimum performance and range at 5-volt operation. Performance will be reduced at maximum and minimum operating voltage.

READER MODULE DIMENSIONS AND PINOUT



ORDERING INFORMATION

Part Number	Description
PirFlx	Raspberry Pi Reader for 125KHz with external antenna

REVISION HISTORY

Version	Date	Comment
V1.0	July 2015	First version.