DATA SHEET

HT RM 310

HITAG™ Mini Reader Module

Preliminary Specification
Revision 2.3

November 1997

PHILIPS

Contents:

1. Introduction

1.1. Features of the Reader Module HT RM310

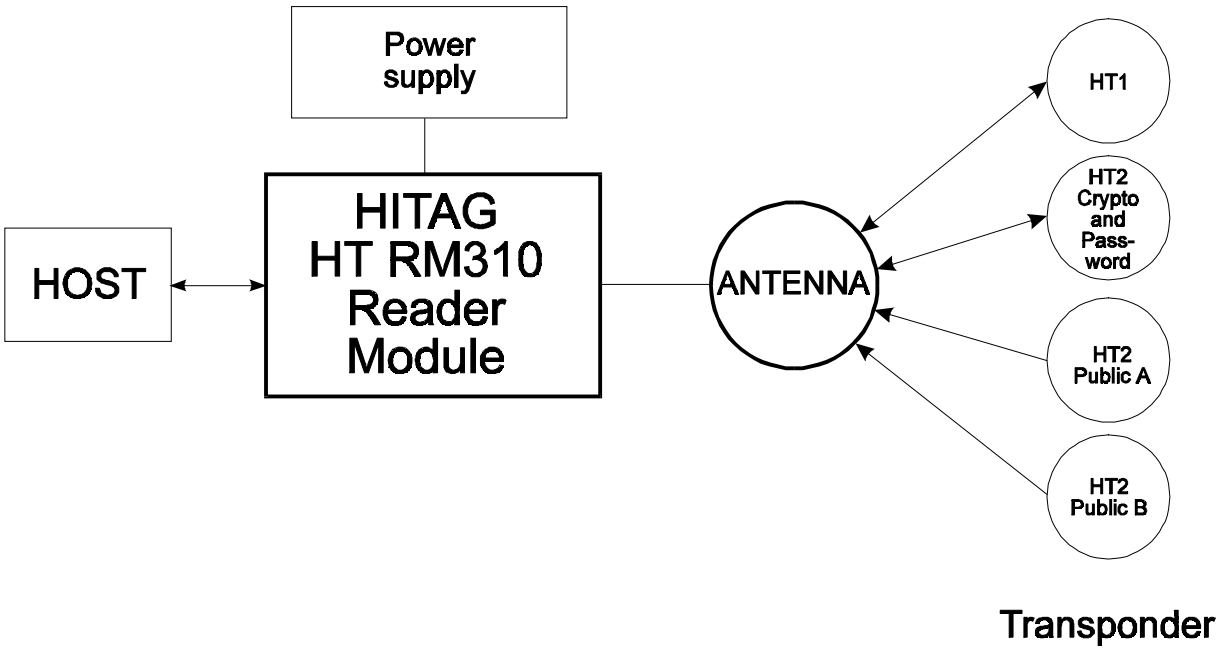
The reader module HT RM310 was designed for reading HITAG 1 and HITAG 2 transponders. It allows universal and cost efficient communication with transponders on a very basic system level. Thanks to the small size of the module it can be easily integrated and used in various applications.

The interface to the host is designed in a rather simple way. It allows fast communication between reader module and transponder, while the user need not take into account analogue signals or the timing of the transponder.
The reader module HT RM310 is suited for all applications requiring proximity operating ranges. By using only a few external components the reader can be easily adapted to a specific read/write device which can be used in various applications.

The reader module HT RM310 has an integrated crypto processor which allows data encryption. The HT RM310 supports the following operating modes:

- HITAG 1 (Plain and Crypto Access)
- HITAG 2 Crypto Mode
- HITAG 2 Password Mode
- HITAG 2 Public Mode A (Standard Read Only transponders structured like a µEM H400x)
- HITAG 2 Public Mode B (Transponders according to ISO Standard 11784 and 11785 for animal identification)

1.2. System Structure



The components shown in the diagram above are required in order to create a complete system with the HT RM310 reader module.

Antennas of different shapes can be connected to the module. The antennas are tuned using a capacitance and optionally a resistor. For detailed information please see Chapter 2.4.

The host system controls all actions of the reader module via a parallel interface.

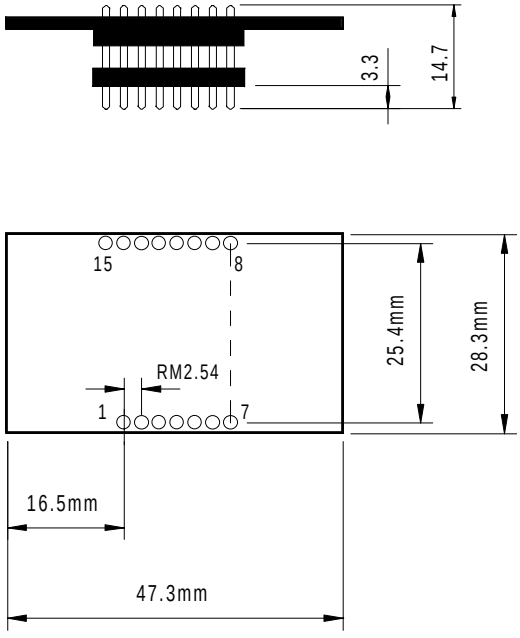
The supply voltage must be a stabilized 5V DC voltage.

2. Technical Data

2.1. General Data

Dimensions (L x W x H)	47.3 x 28.3 x 11.4mm
Supply voltage	5 V DC ± 5 %
Power consumption: • **standard mode** • **energy saving mode**	(depends on the geometry of the antenna) typ. 290 mW 20 mW
Temperature range	-25°C to +70 °C in operation -40°C to +85°C when stored
Antenna	can be connected via the pin connectors
Interface	CMOS 8 Bit parallel + 2 control lines
EEPROM **(HT RM310 only)**	10,000 write cycles

2.2. Dimensions of the HT RM310



2.3. Pin Assignment of the Male Connector

The male connector is divided into two lines. For the pin numbers please refer to the diagram "Dimensions of the HT RM310".

Pin Number	Name	Function
1	/HCDA	Control signal Host data control
2	/RCDA	Control signal Reader data control
3	/MCLR	Reset entry: A reset has to be performed in case of a voltage drop. **Without this precaution, the internal crypto unit might get irreversible damaged.** **(refer to Appendix B)**
4	VCC	5 V Supply voltage *
5	GND	Ground
6	RxA	Antenna - input signal
7	TxA	Antenna - output signal
8	D7	Data Bit 7
9	D6	Data Bit 6
10	D5	Data Bit 5
11	D4	Data Bit 4
12	D3	Data Bit 3
13	D2	Data Bit 2
14	D1	Data Bit 1
15	D0	Data Bit 0

* Only regulated voltage to be used

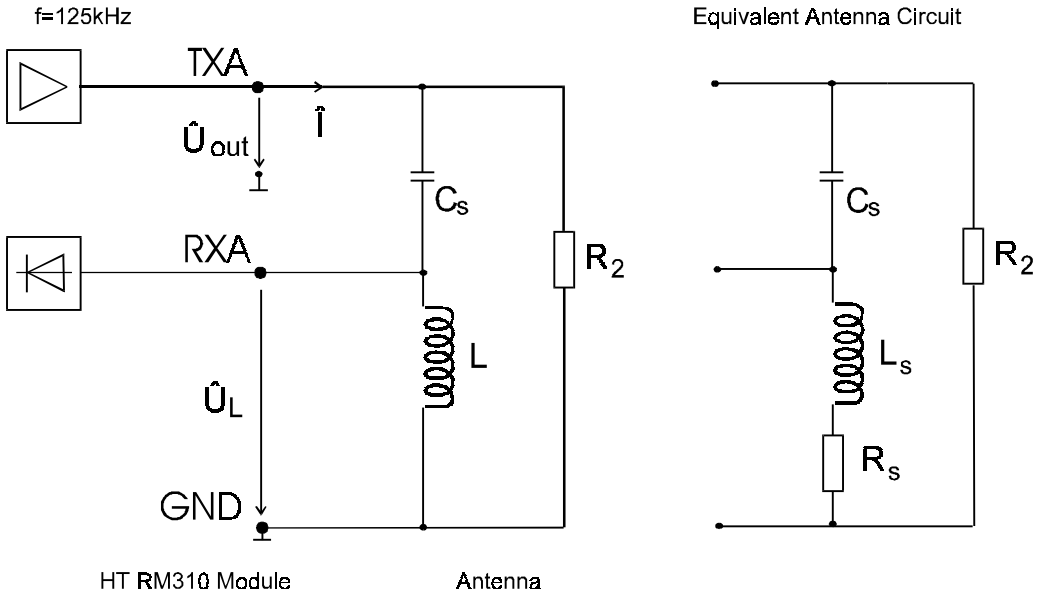
2.4. How to Design Proximity Antennas

The antenna is an important part in the data transmission between the read/write device and the transponder. Thus, when building the antenna the instructions should be strictly followed in order to achieve optimum results.

When deciding upon the size of the antenna the ratio between the diameter of the antenna and the diameter of the transponder´s coil is fundamental. This ratio should be within the limits ranging from 1 to 4. If the ratio is too big or too small, read/write distances may decrease and difficulties during data transmission may occur.

2.4.1. Basics

The following block diagram shows the general structure of a proximity antenna and its connection to the proximity read/write device.



When developing an antenna it is important to take into consideration the limits of the read/write device, i.e. the maximum antenna current and the maximum voltage at the receiver input (Pin RxA). With an output voltage $\hat{U}_{out}$ (Pin TxA) of approximately 2.5Vp the following limits apply to the reader module.

Maximum antenna current ($\hat{I}$)	:	100 mAp
Maximum input voltage (Pin RxA, $\hat{U}_L$)	:	32 Vp

The resistance R2 (approx. 600 ... 1000 Ω) is only needed with cables longer than 50 cm.

2.4.2. Antenna Coil

The inductance of the coil should be in the range of 350 and 500 µH.

The quality factor of the antenna should be approximately Q = 40.

$$Q = \frac{2 \cdot \pi \cdot f \cdot L_S}{R_S}$$

If the Q factor is too high, it must be reduced by using an additional resistor. Generally speaking it is better to have a smaller diameter of the wire for the coil rather than using an additional resistor.

The following equation shows the approximate calculation of the number of coil windings for a required inductance and antenna geometry:

$$L = 2 \cdot a \cdot \ln\left(\frac{a}{D} - K\right) \cdot N^{1.9}$$

The abbreviations read as follows:

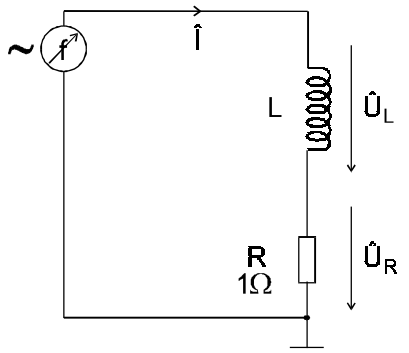
L	required inductance (nH)	
a	circumference of the antenna (cm)	
D	diameter of the wire (cm)	
N	number of windings	
K	geometrical constant	
	circle antenna:	K= 1.01
	square antenna:	K= 1.47

Please note:
The factor K is usually much smaller than the quotient a/D and can thus be neglected.

$$N \approx \sqrt[1,9]{\frac{L}{2 \cdot a \cdot \ln(a/D)}}$$

2.4.3. Measuring Inductance

The inductance of the designed coil can be determined using the following measuring procedure.

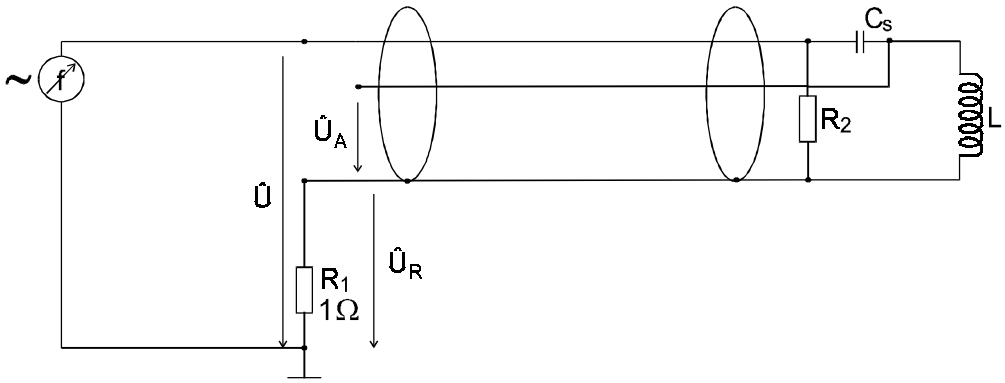


A sinus signal of 125 kHz is supplied by using a function generator. If you measure the current Î and the antenna voltage $\hat{U}_L$, the inductance can be calculated according to the following formula:

$$L = \frac{\hat{U}_L}{\omega \cdot \hat{I}} \qquad \omega = 2 \cdot \pi \cdot f$$

2.4.4. Antenna Tuning

The antenna has to be tuned to its final form by using the connecting cable. You must not change anything with the antenna coil or with the connecting cable, after having finished tuning the antenna. If you do, the mechanical changes will influence the electrical values and the antenna will be detuned again.



A sinus signal of 125 kHz is fed to the antenna connectors using a frequency generator**.** Now you measure the voltages Û and $\hat{U}_R$ with an oscilloscope. Then change the frequency until Û and $\hat{U}_R$ are in phase.

If the resonance frequency achieved is too high, C_S has to be increased. If it is too low, C_S has to be decreased.

The aim is to arrive at a resonance frequency of 125 kHz using C_S.

The phase of impedance has to be in the range of +/- 10°.

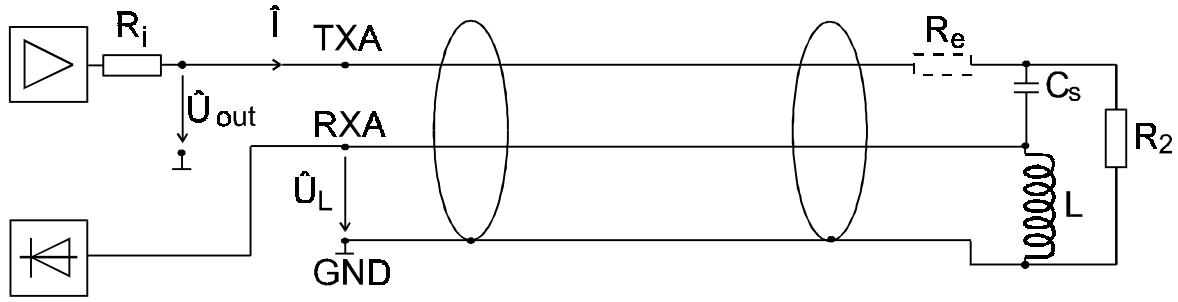
2.4.5. Determining the Serial Resistance of the Antenna

Use an oscilloscope to measure $\hat{U}_A$ and $\hat{U}_R$ at a frequency of 125 kHz.
The serial resistance R_S can be calculated with the following formula:

$$\hat{I} = \frac{\hat{U}_R}{R_1} \qquad \Rightarrow \qquad R_S = \frac{\hat{U}_A}{\hat{I}}$$

2.4.6. Checking the Antenna Voltage $\hat{U}_L$

Before connecting the antenna to the read/write device (as shown in the graph below), you must carry out a check calculation of the input level of the read/write device according to the formula below in order to prevent damage.



$$\hat{I} = \frac{\hat{U}_{out}}{R_i + R_s + (R_e)} \qquad \text{with} \qquad R_i \approx 22\Omega$$

(R_i is the internal resistance of the output amplifier)

$$\hat{U}_{out} \approx 2.5Vp \qquad \hat{U}_L = L \cdot \omega \cdot \hat{I} \qquad \omega = 2 \cdot \pi \cdot f \qquad f = 125kHz$$

The maximum value for $\hat{U}_L$ is 32 Vp. Based on this calculation damage is avoided at the receiver input (Pin RxA) of the read/write device.

With $\hat{U}_L$ < 32 Vp the resistor R_e can be omitted.

With $\hat{U}_L$ > 32 Vp you have to calculate and insert R_e according to the following formula:

$$R_e = L \cdot \omega \cdot \frac{\hat{U}_{out}}{\hat{U}_{L\max}} - R_i - R_s \qquad \Rightarrow \qquad R_e \geq L \cdot \omega \cdot 0{,}078 - R_i - R_s$$

with $R_i \approx 22\Omega$

2.4.7. Procedure for Practical Antenna Design

The procedure how to design a HITAG Proximity antenna has been described in the previous chapters. Generally speaking the following steps have to be considered:

1. The required antenna inductance can be chosen in the range of 350µH and 500µH (e.g. L=420µH).

2. The number of turns N can be calculated with the following formula:

$$N = \sqrt[1,9]{\frac{L[nH]}{2 \cdot a \cdot \ln \cdot (a/D - K)}}$$

   for L=420µH:

$$N = \sqrt[1,9]{\frac{420\,000}{2 \cdot a \cdot \ln \cdot (a/D - K)}} = \frac{633}{\sqrt[1,9]{a \cdot \ln(a/D)}}$$

   Please note:
   Usually the factor K is much smaller than the quotient from a/D and can thus be neglected.

3. Now the antenna can be build according to the required dimensions (circumference a) with the calculated number of turns.

   Please note:
   The antenna coil must not be changed afterwards because with the mechanical dimensions the electrical specifications are changing, too. That means the number of turns, the shape, the arrangement of the coil windings and the antenna supply cable must be used in their final form.

   Please note:
   Metal influences considerably the electric characteristics of the antenna. If metal is close to the antenna when it is set up, all instructions below must be followed (distance from metal < maximum diameter of the antenna).

4. Measuring the inductance L of the antenna is described in Chapter 2.4.3.

5. Determination of the serial capacitor C_S is described in Chapter 2.4.4.

   Please note:
   The capacitance of the antenna supply cable can be determined according to the specifications given in the data sheet of the cable (e.g. Cp = 180 pF/m).

6. Now the antenna has to be tuned according to the instructions given in Chapter 2.4.4.
   The tuning of the antenna is finished when the phase of impedance is within the range of +/- 10°.

7. The serial resistance R_s of the antenna is the impedance of the tuned antenna and is an ohms resistance at the resonance frequency (f=125 kHz). It can be calculated according to the formula given in Chapter 2.4.5.

8. In order to achieve a satisfactory reading distance, the quality factor of the antenna coil (for non-metal environment) should be approximately Q = 40.

   The quality factor of the coil is calculated as follows:

$$Q = \frac{\omega \cdot L}{R_S} = \frac{2 \cdot \pi \cdot f \cdot L}{R_S}$$

9. By knowing R_s and the dropping resistor (R_i = 22Ω) the current $\hat{I}$ and the antenna voltage $\hat{U}_L$ can be calculated. It is very important to calculate the antenna voltage before connecting the antenna to the HT RM310 module to avoid damage. If the calculated value of $\hat{U}_L$ is higher than $\hat{U}_L$ =32 Vp, a resistor R_e must be used to protect the receiver input.
   The resistor has to be placed as shown in Chapter 2.4.6.

10. After having checked the antenna voltage as described in point 9, connect your antenna to the HT RM310 module and measure the read/write distances with your transponders. Should the read/write distances not meet your expectations, the following points should be considered:

- The size of the antenna and the size of the transponder have to be in a defined ratio (between 4 and 1).
  That means if you increase the antenna beyond a certain size, the maximum read/write distances will decrease when using the same transponder.

- The optimal shape of the antenna coil is a circle, while the performance of a square shaped coil is much better than that of a rectangular one (with the same circumference).

- In order to achieve better read/write distances the quality factor of the antenna coil should be increased, but must not be higher than Q=40. This can be attained with the following measures:

– All conducting material has to be removed from the antenna environment.
– A thicker wire can be used for the coil.
– Ferrite can be placed behind the antenna coil to concentrate the field.
– Extension of the antenna area.
– Also with a different number of turns better results can be achieved.

Attention:
The above measures must not differ from the antenna design instructions of Chapter 2.4.

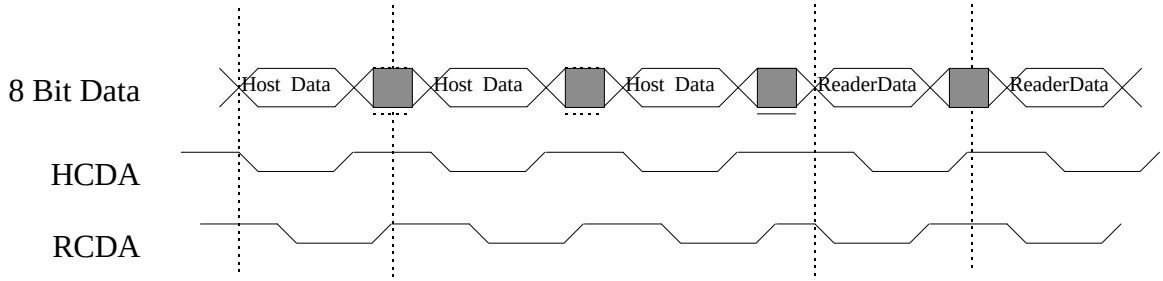
3. Interface HT RM310 ⇔ Host

Communication with the host is carried out via an 8 Bit parallel interface with two control lines.

3.1. General Definitions

3.1.1. Hardware

The interface needs in total 10 lines (8 data lines and 2 control lines). The data lines are bi-directional, while the control lines are unidirectional. The control lines from host to reader module (host control data /HCDA) and from reader module to host (reader control data /RCDA) are low active. By activating the control line either the host or the reader module indicate that data is on the data line. The respective counter part sets its control line to LOW for a short period of time, while the rising ramp of the control line indicates that the data transmission has been finished.



Graph: Timing diagram

A bus conflict can never occur, since communication is always initiated by the host. The reader module responds upon the request command of the host, while the host has to wait for the response of the reader module. If the reader module does not respond within the specified time of 1s for this command (see appendix A: Timing Interface), a time out occurs and the host starts again with a request.

Since both the host and the reader module can send data, the data lines should only be operated when also the respective control line indicates data.

3.1.2. Structure of the Protocol

The protocol is structured according to the following format:

Byte	1	2	...	n-1
Function	Command/Status	Data	...	Data

Command / Status	Contains either the command number of the command to be executed or the status message for the command to be executed. Please refer to the appendix for the structure of the command/status byte.
Data	Data is transmitted binary, that means characters between 0x00 and 0xFF are allowed. Data is only transmitted when the command requires the transmission of data.

3.2. Set of Commands

The commands can be divided into five different sets:

1) HITAG 1 Read/Write Commands
2) HITAG 2 Read/Write Commands
3) Public Mode Read Commands
4) General Commands
5) Commands for Personalization

3.2.1. HITAG 1 Read/Write Commands

Name of command	Function
GetSnr_HT1	Reads serial number
GetSnr_HT1_A	Reads serial number in advanced mode
SelectSnr_HT1	Selects transponder
SelectLastSnr_HT1	Selects transponder with serial number read with last GetSnr_HT1
HaltSelected_HT1	Sets transponder in halt mode
ReadPage_HT1_P	Reads a page in plain mode
ReadPage_HT1_C	Reads a page in encrypted mode
WritePage_HT1_P	Writes a page in plain mode
WritePage_HT1_C	Writes a page in encrypted mode
ReadBlock_HT1_P	Reads a block in plain mode
ReadBlock_HT1_C	Reads a block in encrypted mode
WriteBlock_HT1_P	Writes a block in plain mode
WriteBlock_HT1_C	Writes a block in encrypted mode
MutualAuthent_HT1	Carries out a full authentication procedure

3.2.2. HITAG 2 Read/Write Commands

Name of command	Function
GetSnr_HT2_P	Selects transponder and reads serial number in Password Mode
GetSnr_HT2_C	Selects transponder and reads serial number in Crypto Mode
HaltSelected_HT2	Sets transponder in halt mode
ReadPage_HT2	Reads a page
ReadPageInv_HT2	Reads a Bit inverted page
WritePage_HT2	Writes a page (with single inversion of the address)

3.2.3. Public Modes

Name of command	Function
ReadPublic A	Reads Page 4 and 5 of HT2 in Public Mode A
ReadPublic B	Reads Page 4 to 7 of HT2 in Public Mode B

3.2.4. General Commands

Name of command	Function
HF_OFF	Deactivates the RF field. The RF field is activated with any command or with each LOW signal generated by /HCDA.
Power Down	Sets the entire module into sleep mode. The sleep mode is deactivated by any command or LOW signal of /HCDA.
GetVersion	Displays the software version.

3.2.5. Commands for Personalization

Name of command	Function
WriteSecret_HT	Writes Keys, Logdata and Password into the EEPROM.

3.3. Description of the Commands

3.3.1. GetSnr_HT1

This command reads the serial number of a HITAG 1 transponder in “Standard Protocol Mode“.

Protocol:

Host - Reader module

0x10

Reader module - Host

status
Snr [0]
Snr [3]

status: 0 no error
1 INTERFACE error
3 NOTAG error

3.3.2. GetSnr_HT1_Adv

This command reads the serial number of a HITAG 1 transponder and switches the transponder into “Advanced Protocol Mode“. The transponder now responds on all commands in the “Advanced Protocol Mode“. This mode can only be left by an “power on reset“ of the transponder (use “HF_OFF“ or “Power Down“ command or move the transponder out of the antenna field). The “Advanced Protocol Mode“ is not left by using the “GetSnr_HT1“.
The major difference between “Standard Protocol Mode“ and “Advanced Protocol Mode“ is increased data reliability during data transmission from the transponder to the reader by using an 8 Bit CRC and a longer start sequence.
The “Advanced Protocol Mode“ is not supported by transponder version HT1 ICS30 0***1***x, but only by version HT1 ICS30 0***2***x with serial numbers 0x y***5***yyyyyy

Protocol:

Host - Reader module

0x11

Reader module - Host

status
Snr [0]
Snr [3]

status: 0 no error
1 INTERFACE error
3 NOTAG error

3.3.3. SelectSnr_HT1

This command selects a HITAG 1 transponder with the serial number given in the protocol. With this selection the transponder is prepared for read and write commands in HITAG 1 mode.
The command provides the OTP of the selected transponder. Using the "Advanced Protocol Mode" of HITAG 1 transponders by using the "GetSnr_HT1_Adv" command the data is followed by an 8 Bit CRC.

Protocol:

Host - Reader module

0x12
Snr [0]
Snr [3]

Reader module - Host

status
OTP [0] LSB
OTP [3] MSB

status: 0 no error
1 INTERFACE error
3 NOTAG error

3.3.4. SelectLastSnr_HT1

This command selects a HITAG 1 transponder with the serial number read by the last error free command "GetSnr_HT1". There must be no reset of the transponder (caused by the commands "HF-OFF", "Powerdown" or by moving the transponder out of the antenna field) between the commands "GetSnr_HT1" and "SelectLastSnr_HT1"
With this selection the transponder is prepared for read and write commands in HITAG 1 mode.
The command provides the OTP of the selected transponder. In the "Advanced Protocol Mode" of HITAG 1 transponders (by using the "GetSnr_HT1_Adv"-command) the data is followed by an 8 Bit CRC.

Protocol:

Host - Reader module

0x13

Reader module - Host

status
OTP [0] LSB
OTP [3] MSB

status: 0 no error
1 INTERFACE error
3 NOTAG error

3.3.5. HaltSelected_HT1

Sets the selected transponder in halt mode, i.e. the transponder is muted until it has left the RF field or until the RF field is deactivated. By using this command different transponders can be handled simultaneously in the operating field of the antenna.

Protocol:

Host - Reader module

0x14

Reader module - Host

status

status: 0 no error
1 INTERFACE error
8 ACKNOWLEDGEMENT error

3.3.6. ReadPage_HT1_P / ReadPage_HT1_C

Reads a page of the selected transponder.
The command “ReadPage_HT1_P“ reads plain areas of the HITAG 1 transponders only.
Reading encrypted areas of the HITAG 1 transponder with this command leads to a status “NOTAG error“ and the transponder is reset.

To read encrypted areas of the transponders use the command “ReadPage_HT1_C“.
Access to the secret area is only possible in Crypto Mode after a mutual authentication.

In the “Advanced Protocol Mode“ of HITAG 1 transponders (by using the “GetSnr_HT1_Adv“-command) the data is followed by an 8 Bit CRC.

Protocol:

Host - Reader module

0x15 / 0x16
pagenr

Reader module - Host

status
data[0]
data[3]

status: 0 no error
1 INTERFACE error
3 NOTAG error
9 CRYPTOBLOCK NOT INIT

3.3.7. ReadBlock_HT1_P / ReadBlock_HT1_C

Reads a block (up to 4 pages) of the selected transponder.
The command “ReadBlock_HT1_P“ reads plain areas of the HITAG 1 transponders only.
Reading encrypted areas of the HITAG 1 transponder with this command leads to a status “NOTAG error“ and the transponder is reset.

To read encrypted areas of the transponders use the command “ReadBlock_HT1_C“.
Access to the secret area is only possible in Crypto Mode after a mutual authentication.

In the “Advanced Protocol Mode“ of HITAG 1 transponders (by using the “GetSnr_HT1_Adv“-command) the data is followed by an 8 Bit CRC.
With the command ”ReadBlock_HT1_P“ resp. ”ReadBlock_HT1_C“ data beginning from the start address (page number) till the end of the block can be read. Depending on the start address 4, 8, 12 or 16 Bytes are provided by the reader module.

Protocol:

Host - Reader module

0x17 / 0x18
pagenr

Reader module - Host

status
data[0]
data[n]

n = 4, 8, 12, 16

status: 0 no error
1 INTERFACE error
3 NOTAG error
9 CRYPTOBLOCK NOT INIT

3.3.8. WritePage_HT1_P / WritePage_HT1_C

Writes a page of the selected transponder.
Writing to encrypted areas of the HITAG 1 transponder with this command leads to a status "NOTAG error" and the transponder is reset.

To write to encrypted areas of the transponders use the command "WritePage_HT1_C".
Access to the secret area is only possible in Crypto Mode after a mutual authentication.

Upon completion of the write command, a "Read after Write" procedure should be carried out in order to check whether the write access was successful.

Protocol:

Host - Reader module

0x19 /0x1A
pagenr
data[0] data[3]

Reader module - Host

status

status: 0 no error
1 INTERFACE error
3 NOTAG error
4 TIMEOUT error
9 CRYPTOBLOCK NOT INIT

3.3.9. WriteBlock_HT1_P / Write Block_HT1_C

Writes a block (up to 4 pages) of the selected transponder.
Writing to encrypted areas of the HITAG 1 transponder with this command leads to a status "NOTAG error" and the transponder is reset.

To write to encrypted areas of the transponders use the command "WriteBlock_HT1_C".
Access to the secret area is only possible in Crypto Mode after a mutual authentication.

With the command "WriteBlock_HT1_P" resp. "WriteBlock_HT1_C" data beginning from the start address (page number) till the end of the block can be written. Depending on the start address 4, 8, 12 or 16 Bytes are written with one command to the transponder.
Upon completion of the write command, a "Read after Write" procedure should be carried out in order to check whether the write access was successful.

Protocol:

Host - Reader module

0x1B / 0x1C
pagenr
data[0]
data[n]

n = 4, 8, 12, 16

Reader module - Host

status

status: 0 no error
1 INTERFACE error
3 NOTAG error
4 TIMEOUT error
9 CRYPTOBLOCK NOT INIT

3.3.10. MutualAuthent_HT1

This command carries out the full authentication procedure of the transponder and the reader module.
After this authentication areas in encrypted mode can be accessed resp. encrypted commands can be used in the communication with the transponder.
The transponder exits encrypted mode if a not encrypted command, a “GetSnr_HT1“ or “GetSnr_HT1_Adv“ command is used or if the transponder is reset (caused by the commands “HF-OFF“, “Powerdown“ or by moving the transponder out of the antenna field).
Using the Byte “loginfo“ you can choose between Log information (Keys and Logdata) A or B

Protocol:

Host - Reader module

0x1D
loginfo

loginfo: 0x00 loginfo A
0x02 loginfo B

Reader module - Host

status

status: 0 no error
1 INTERFACE error
7 AUTHENT error

3.3.11. GetSnr_HT2_P

This command selects a HITAG 2 transponder in Password Mode. With this selection the transponder is prepared for read and write commands in HITAG 2 Password Mode.
For the selection in Password Mode, a password is transmitted to the reader module which must correspond to Page 1 on the transponder (Password RWD). After the command has been executed, the reader module returns the serial number and the content of Page 3 (configbyte with 24 Bit Password TAG).
When the transponder is in Crypto Mode, no selection occurs and only the serial number and the status message "Password RWD error" are returned.

If the transponder is set in one of the public modes, it can only be selected within 2.56 ms after reset (entering the RF field or activating the RF field).

Protocol:

Host - Reader module

0x0A
Password [0] Password [3]

Reader module - Host

status
Snr [0] Snr [3]
configbyte
Password TAG [0] Password TAG [2]

status: 0 no error
1 INTERFACE error
3 NOTAG error
5 PASSWORD RWD error

3.3.12. GetSnr_HT2_C

This command selects a HITAG 2 transponder in Crypto Mode. With this selection the transponder is prepared for read and write commands in HITAG 2 Crypto Mode.

After the command has been executed, the reader module returns the serial number and the content of the configbyte.

When a transponder in Password Mode receives the command "GetSnr_HT2_C", only the serial number and the status message "Password RWD error" are returned.

If the transponder is set in one of the public modes, it can only be selected within 2.56 ms after reset (entering the RF field or activating the RF field).

Protocol:

Host - Reader module

0x0B

Reader module - Host

status
Snr [0] Snr [3]
configbyte
Password TAG [0] Password TAG [2]

status: 0 no error
1 INTERFACE error
3 NOTAG error
7 AUTHENT error

3.3.13. HaltSelected_HT2

Sets the selected transponder in halt mode, i.e. the transponder is muted until it has left the RF field or until the RF field is deactivated. By using this command different transponders can be handled simultaneously in the operating field of the antenna.

Protocol:

Host - Reader module

0x0C

Reader module - Host

status

status: 0 no error
1 INTERFACE error
8 ACKNOWLEDGEMENT error

3.3.14. ReadPage_HT2

Reads a page of the selected transponder. In order to increase data security this command should always be combined with the command ReadPageInv_HT2. Then the data which has been read with ReadPage_HT2 and ReadPageInv_HT2 should be compared with each other.

Protocol:

Host - Reader module

0x0D
pagenr

Reader module - Host

status
data [0] data [3]

status: 0 no error
1 INTERFACE error
3 NOTAG error

3.3.15. ReadPageInv_HT2

Reads a Bit inverted page of the selected transponder. This command increases the data security and should always be combined with the command ReadPage_HT2. Then the data which has been read with ReadPageInv_HT2 and ReadPage_HT2 should be compared with each other.

Protocol:

Host - Reader module

0x0E
pagenr

Reader module - Host

status
data [0] data [3]

status: 0 no error
1 INTERFACE error
3 NOTAG error

3.3.16. WritePage_HT2

Writes a page of the selected transponder.
Upon completion of the write command, "Read after Write" should be carried out in order to check whether the write command was successful.

Please note: The address is transmitted both non-inverted and inverted to the transponder.

Protocol:

Host - Reader module

0x0F
pagenr
data [0] data [3]

Reader module - Host

status

status: 0 no error
1 INTERFACE error
3 NOTAG error
4 TIMEOUT error

3.3.17. ReadPublic A

Reads a transponder in Public A Mode. The coding of the data area must contain a header and the parity structure of the µEM H400x. Only the 40 Bit (5 byte) information of the µEM H400x data (1 byte customer ID; 4 byte user ID) is transmitted.

Protocol:

Host - Reader module

0x07

Reader module - Host

status
customer ID
user ID [0] user ID [3]

status: 0 no error
1 INTERFACE error

3.3.18. ReadPublic B

Reads a transponder in Public B Mode. The coding of the data areas must, however, have a header according to ISO 11785. 13 byte (8 byte identification code, 2 byte CRC, 3 byte extension) are transmitted.

Protocol:

Host - Reader module

0x08

Reader module - Host

status
data [0] data [7]
CRC [0] CRC [1]
Extension [0] Extension [2]

status: 0 no error
1 INTERFACE error

3.3.19. HF-OFF

Deactivates the RF field of the antenna. When receiving the next command (/HCDA) the RF field is automatically activated again.

Protocol:

Host - Reader module	0x01
Reader module - Host	status

status: 0 no error
1 INTERFACE error

3.3.20. Powerdown

This command sets the complete reader module into sleep mode. When receiving the next command (/HCDA) the reader module is automatically set into operating mode.

Protocol:

Host - Reader module	0x02
Reader module - Host	status

status: 0 no error
1 INTERFACE error

3.3.21. GetVersion

Reads the software version of the reader module.

Protocol:

Host - Reader module	0x03

Reader module - Host

status
Version - overview Version - in detail
reserved reserved

status: 0 no error
1 INTERFACE error

3.3.22. WriteSecret_HT

Using this command the reader module receives the data needed for the secret access to the HITAG transponders. The data is stored "write only" in the internal EEPROM of the Crypto Processor.
In order to change the data, the value of the current data has to be transmitted first to the reader module. The individual data areas of the secret access data are changed one after another and the module returnes ***"no error"*** statusbytes(0x00) for each matching data couple (old and new data).
The personalization process is interrupted if the comparison of old and new data prove inconsistent. The module then returnes the according status for the data couple that does not match.

Please Note : To successfully change the secret data you have to complete the whole procedure step by step as shown in the following protocol description.
In case of an error the host has to cancel the personalization procedure.

Protocol:

Host - Reader module

0x00
old Key A [0] old Key A [3]
new Key A [0] new Key A [3]

Reader module - Host

status

status: 0 no error
1 INTERFACE error
80 Wrong Crypto
81 Wrong old Key A

Host - Reader module

0x00
old Key B [0] old Key B [3]
new Key B [0] new Key B [3]

Reader module - Host

status

status: 0 no error
1 INTERFACE error
80 Wrong Crypto
82 Wrong old Key B

Host - Reader module

0x00
old Logdata 0A [0] old Logdata 0A [3]
new Logdata 0A [0] new Logdata 0A [3]

Reader module - Host

status

status: 0 no error
1 INTERFACE error
80 Wrong Crypto
83 Wrong old Logdata 0A

Host - Reader module

0x00
old Logdata 0B [0] old Logdata 0B [3]
new Logdata 0B [0] new Logdata 0B [3]

Reader module - Host

status

status: 0 no error
1 INTERFACE error
80 Wrong Crypto
84 Wrong old Logdata 0B

Host - Reader module

0x00
old Logdata 1A [0] old Logdata 1A [3]
new Logdata 1A [0] new Logdata 1A [3]

Reader module - Host

status

status: 0 no error
1 INTERFACE error
80 Wrong Crypto
85 Wrong old Logdata 1A

Host - Reader module

0x00
old Logdata 1B [0] old Logdata 1B [3]
new Logdata 1B [0] new Logdata 1B [3]

Reader module - Host

status

status: 0 no error
1 INTERFACE error
80 Wrong Crypto
86 Wrong old Logdata 1B

Host - Reader module

0x00
old HT2 Key 16 [0] old HT2 Key 16 [3]
new HT2 Key 16 [0] new HT2 Key 16 [3]

Reader module - Host

status

status: 0 no error
1 INTERFACE error
80 Wrong Crypto
87 Wrong old HITAG 2 Key 16

Host - Reader module

0x00
old HT2 Key 32 [0] old HT2 Key 32 [3]
new HT2 Key 32 [0] new HT2 Key 32 [3]

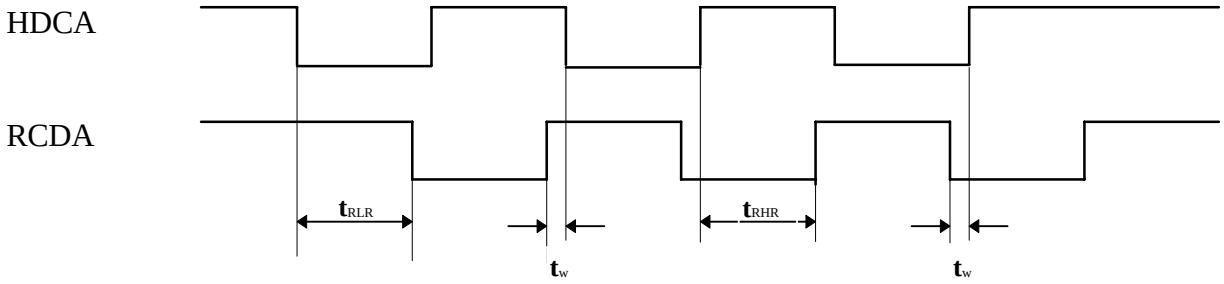
Reader module - Host

status

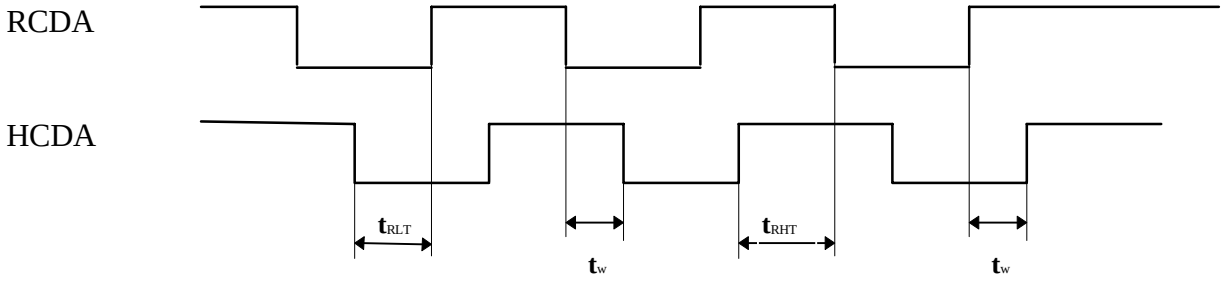
status: 0 no error
1 INTERFACE error
80 Wrong Crypto
88 Wrong old HITAG 2 Key 32

4. Appendix A: Timing Interface

Host → HT RM310-Module (Receive Mode):



HT RM310-Module → Host (Transmit Mode):

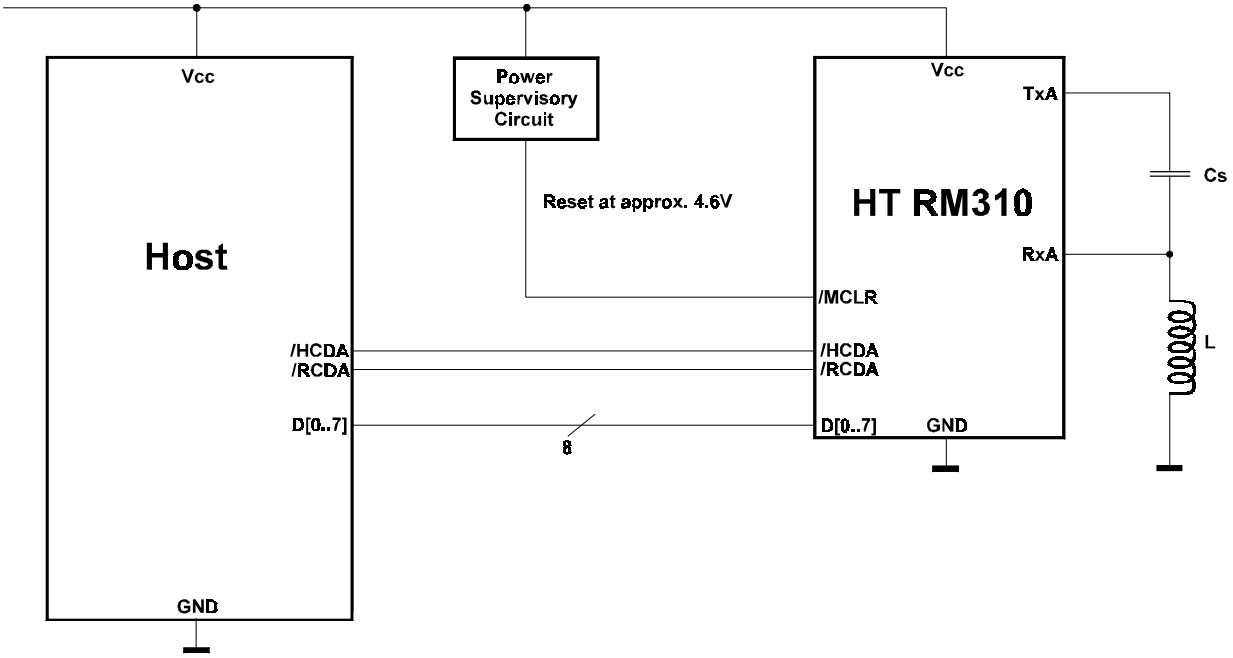


Time	Description	min.	typ.	max.
t_{RLR}	wait for RCDA Low in Receive Mode		25 µs	1 s
t_{RHR}	wait for RCDA High in Receive Mode		17 µs	1 s
t_{RLT}	wait for RCDA Low in Transmit Mode		15 µs	
t_{RHT}	wait for RCDA High in Transmit Mode		20 µs	
tw	wait for Host	5µs		50 ms

Note: The max. time corresponds to the time-out

5. Appendix B: Application Example

The figure below shows an example of a standard application with the HT RM310 Mini Reader Module connected to a host.
To avoid destruction of the internal EEPROM data in case of powerfailure a power supervisory circuit to monitor the supply voltage is required.



6. Appendix C: Reaction Times of the Reader Module

Action	min.	typ.	max.	unit
GetSnr_HT2_P	3 [1)]		36 [2)]	ms
ReadPage_HT2		16,5		ms
WritePage_HT2	23		25	ms
Halt_HT2		10,5		ms
GetSnr_HT2_C	3[1)]		98	ms
ReadPage_HT2 (Crypto)		32		ms
WritePage_HT2 (Crypto)		43		ms
Halt_HT2 (Crypto)		18		ms
WriteSecret_HT		425		ms
Read Public Mode A [3)]	33		65	ms
Read Public Mode B [3)]	40		70	ms
GetSnr_HT1	3,5 [1)]		22 [2)]	ms
GetSnr_HT1_A	3,5 [1)]		23 [2)]	ms
SelectSnr_HT1 (Standard)		21		ms
SelectSnr_HT1 (Advanced)		25		ms
SelectLastSnr_HT1 (Standard)		21		ms
SelectLastSnr_HT1 (Advanced)		25		ms
HaltSelected_HT1 (Standard)		9		ms
HaltSelected_HT1 (Advanced)		10		ms
ReadPage_HT1_P (Standard)		16,5		ms
ReadPage_HT1_P (Advanced)		20		ms
ReadPage_HT1_C (Standard)		32,5		ms
ReadPage_HT1_C (Advanced)		38,5		ms
ReadBlock_HT1_P (Standard) [4)]		41		ms
ReadBlock_HT1_P (Advanced) [4)]		45,5		ms
ReadBlock_HT1_C (Standard) [4)]		86		ms
ReadBlock_HT1_C (Advanced) [4)]		94		ms
WritePage_HT1_P (Standard)	28		30	ms
WritePage_HT1_P (Advanced)	29		31	ms
WritePage_HT1_C (Standard)		45		ms
WritePage_HT1_C (Advanced)		49		ms
WriteBlock_HT1_P (Standard) [4)]	85		92	ms
WriteBlock_HT1_P (Advanced) [4)]	87		94	ms
WriteBlock_HT1_C (Standard) [4)]		144		ms
WriteBlock_HT1_C (Advanced) [4)]		146		ms
MutualAuthent_HT1 (Standard)		70		ms
MutualAuthent_HT1 (Advanced)		74		ms

1) no transponder in antenna field
2) transponder in antenna field
3) transponder already in antenna filed
4) 4 Pages

Timing for HITAG 1 is valid for HT1 ICS30 with serial numbers 0x y5yyyyyy only.

7. Appendix D: List of Command Bytes

Hex Value	Command
0x00	WriteSecret_HT
0x01	HF_OFF
0x02	Power down
0x03	GetVersion
0x07	ReadPublic A
0x08	ReadPublic B
0x0A	GetSnr_HT2_P
0x0B	GetSnr_HT2_C
0x0C	HaltSelected_HT2
0x0D	ReadPage_HT2
0x0E	ReadPageInv_HT2
0x0F	WritePage_HT2
0x10	GetSnr_HT1
0x11	GetSnr_HT1_A
0x12	SelectSnr_HT1
0x13	SelectLastSnr_HT1
0x14	HaltSelected_HT1
0x15	ReadPage_HT1_P
0x16	ReadPage_HT1_C
0x17	ReadBlock_HT1_P
0x18	ReadBlock_HT1_C
0x19	WritePage_HT1_P
0x1A	WritePage_HT1_C
0x1B	WriteBlock_HT1_P
0x1C	WriteBlock_HT1_C
0x1D	MutualAuthent_HT1

8. Appendix E: List of Status Bytes

Hex Value	Status
0x00	no error
0x01	Interface error
0x03	NOTAG error
0x04	TIMEOUT error
0x05	Password RWD error
0x07	AUTHENT error
0x08	ACKNOWLEDGEMENT error
0x09	CRYPTOBLOCK NOT INIT
0x80	Wrong crypto
0x81	Wrong old Key A
0x82	Wrong old Key B
0x83	Wrong old Logdata 0A
0x84	Wrong old Logdata 0B
0x85	Wrong old Logdata 1A
0x86	Wrong old Logdata 1B
0x87	Wrong old Key 16
0x88	Wrong old Key 32

Meaning of the status bytes:

no error:	Command executed correctly.
INTERFACE error:	– No proper communication between reader module and host. – Unknown command byte.
NOTAG error:	No transponder in the antenna field or transponder already selected.
TIMEOUT error:	Transponder out of writing distance, not enough energy to write on the transponder.
PASSWORD RWD error:	HT2 was accessed using a wrong Password RWD.
AUTHENT error:	An error occurred during the authentication process. – Keys or Logdata of the transponder and the crypto processor prove inconsistent. – faulty crypto processor. – no crypto processor existing.
ACKNOWLEDGEMENT error:	The acknowledgement of the transponder on a HALT-command was not received correctly.
CRYPTOBLOCK NOT INIT	A cryptographic command was transmitted without authentication.
Wrong Crypto:	Faulty crypto processor. This status is returned only after the personalization command. All other commands return "AUTHENT error".
Wrong old Key A:	Error writing Key A (on comparison old data and new data prove inconsistent)
Wrong old Key B:	Error writing Key B
Wrong old Logdata 0A:	Error writing Logdata 0A
Wrong old Logdata 0B:	Error writing Logdata 0B
Wrong old Logdata 1A:	Error writing Logdata 1A
Wrong old Logdata 1B:	Error writing Logdata 1B
Wrong old HT2 Key 16:	Error writing Key 16
Wrong old HT2 Key 32:	Error writing Key 32

9. Appendix F: List of KEYS in the Crypto Processor

The crypto processor is delivered with the following key set:

Secret Data	Hex Value			
HT1 Key A	00	00	00	00
HT1 Key B	00	00	00	00
HT1 Logdata 0A	00	00	00	00
HT1 Logdata 0B	00	00	00	00
HT1 Logdata 1A	00	00	00	00
HT1 Logdata 1B	00	00	00	00
HT2 Key 16	20	20	4F	4E
HT2 Key 32	4D	49	4B	52

Philips Semiconductors - a worldwide company

Argentina: see South America
Australia: 34 Waterloo Road, NORTHRYDE, NSW 2113,
Tel. +612 9805 4455, Fax. +612 9805 4466
Austria: Computerstraße 6, A-1101 WIEN, P.O.Box 213,
Tel. +431 60 101, Fax. +431 30 101 1210
Belarus: Hotel Minsk Business Centre, Bld. 3, r.1211, Volodarski Str. 6,
220050 MINSK, Tel. +375172 200 733, Fax. +375172 200 773
Belgium: see The Netherlands
Brazil: see South America
Bulgaria: Philips Bulgaria Ltd., Energoproject, 15th floor,
51 James Bourchier Blvd., 1407 SOFIA
Tel. +3592 689 211, Fax. +3592 689 102
Canada: Philips Semiconductors/Components,
Tel. +1800 234 7381
China/Hong Kong: 501 Hong Kong Industrial Technology Centre,
72 Tat Chee Avenue, Kowloon Tong, HONG KONG,
Tel. +85223 19 7888, Fax. +85223 19 7700
Colombia: see South America
Czech Republic: see Austria
Denmark: Prags Boulevard 80, PB 1919, DK-2300 COPENHAGEN S,
Tel. +4532 88 2636, Fax. +4531 57 1949
Finland: Sinikalliontie 3, FIN-02630 ESPOO,
Tel. +3589 61 5800, Fax. +3589 61 580/xxx
France: 4 Rue du Port-aux-Vins, BP 317, 92156 SURESNES Cedex,
Tel. +331 40 99 6161, Fax. +331 40 99 6427
Germany: Hammerbrookstraße 69, D-20097 HAMBURG,
Tel. +4940 23 53 60, Fax. +4940 23 536 300
Greece: No. 15, 25th March Street, GR 17778 TAVROS/ATHENS,
Tel. +301 4894 339/239, Fax. +301 4814 240
Hungary: see Austria
India: Philips INDIA Ltd., Shivsagar Estate, A Block, Dr. Annie Besant Rd.
Worli, MUMBAI 400018, Tel. +9122 4938 541, Fax. +9122 4938 722
Indonesia: see Singapore
Ireland: Newstead, Clonskeagh, DUBLIN 14,
Tel. +3531 7640 000, Fax. +3531 7640 200
Israel: RAPAC Electronics, 7 Kehilat Saloniki St., TEL AVIV 61180,
Tel. +9723 645 0444, Fax. +9723 649 1007
Italy: Philips Semiconductors, Piazza IV Novembre 3,
20124 MILANO, Tel. +392 6752 2531, Fax. +392 6752 2557
Japan: Philips Bldg. 13-37, Kohnan 2-chome, Minato-ku, TOKYO 108,
Tel. +813 3740 5130,Fax. +813 3740 5077
Korea: Philips House, 260-199, Itaewon-dong, Yonsan-ku, SEOUL,
Tel. +822 709 1412, Fax. +822 709 1415
Malaysia: No. 76 Jalan Universiti, 46200 PETALING JAYA, Selangor,
Tel. +60 3750 5214, Fax. +603 757 4880
Mexico: 5900 Gateway East, Suite 200, EL PASO, Texas 79905,
Tel. +9 5800 234 7381
Middle East: see Italy
Netherlands: Postbus 90050, 5600 PB EINDHOVEN, Bldg. VB,
Tel. +3140 27 82785, Fax +3140 27 88399
New Zealand: 2 Wagener Place, C.P.O. Box 1041, AUCKLAND,
Tel. +649 849 4160, Fax. +649 849 7811
Norway: Box 1, Manglerud 0612, OSLO,
Tel. +4722 74 8000, Fax. +4722 74 8341
Philippines: Philips Semiconductors Philippines Inc.,
106 Valero St. Salcedo Village, P.O.Box 2108 MCC, MAKATI,
Metro MANILA, Tel. +632 816 6380, Fax. +632 817 3474
Poland: Ul. Lukiska 10, PL 04-123 WARSZWA,
Tel. +4822 612 2831, Fax. +4822 612 2327
Portugal: see Spain
Romania: see Italy
Russia: Philips Russia, Ul. Usatcheva 35A, 119048 MOSCOW,
Tel. +7095 247 9145, Fax. +7095 247 9144
Singapore: Lorong 1, Toa Payoh, SINGAPORE 1231,
Tel. +65350 2538, Fax. +65251 6500
Slovakia: see Austria
Slovenia: see Italy
South Africa: S.A. Philips Pty Ltd., 195-215 Main Road Martindale,
2092 JOHANNESBURG, P.O.Box 7430 Johannesburg 2000,
Tel. +2711 470 5911, Fax. +2711 470 5494
South America: Rua do Rocio 220, 5th floor, Suite 51,
04552-903 Sao Paulo, SAO PAULO - SP, Brazil,
Tel. +5511 821 2333, Fax. +5511 829 1849
Spain: Balmes 22, 08007 BARCELONA,
Tel. +343 301 6312, Fax. +343 301 4107
Sweden: Kottbygatan 7, Akalla, S-16485 STOCKHOLM,
Tel. +468 632 2000, Fax. +468 632 2745
Switzerland: Allmendstraße 140, CH-8027 ZÜRICH,
Tel. +411 488 2686, Fax. +411 481 7730
Taiwan: Philips Taiwan Ltd., 2330F, 66,
Chung Hsiao West Road, Sec. 1, P.O.Box 22978,
TAIPEI 100, Tel. +8862 382 4443, Fax. +8862 382 4444
Thailand: Philips Electronics (Thailand) Ltd.,
209/2 Sanpavuth-Bangna Road Prakanong, BANGKOK 10260,
Tel. +662 745 4090, Fax. +662 398 0793
Turkey: Talapasa Cad. No. 5, 80640 GÜLTEPE/ISTANBUL,
Tel. +90212 279 2770, Fax. +90212 282 6707
Ukraine: Philips Ukraine, 4 Patrice Lumumba Str., Building B, Floor 7,
252042 KIEV, Tel. +38044 264 2776, Fax. +38044 268 0461
United Kingdom: Philips Semiconductors Ltd., 276 Bath Road, Hayes,
MIDDLESEX UM3 5BX, Tel. +44181 730 5000, Fax. +44181 754 8421
United States: 811 Argues Avenue, SUNNYVALE, CA94088-3409,
Tel. +1800 234 7381
Uruguay: see South America
Vietnam: see Singapore
Yugoslavia: Philips, Trg N. Pasica 5/v, 11000 BEOGRAD,
Tel. +38111 625 344, Fax. +38111 635 777

Philips Semiconductors, Mikron-Weg 1, A-8101 Gratkorn, Austria Fax: +43 / 3124 / 299 - 270

For all other countries apply to: Philips Semiconductors, Marketing & Sales Communications,
Building BE-p, P.O.Box 218, 5600 MD EINDHOVEN, The Netherlands, Fax: +3140 27 24825

Internet: http://www.semiconductors.philips.com/identification

SCB52

PHILIPS