DATA SHEET

HT1 Transponder Family

Communication Protocol
Reader ⇔ HITAG™1 Transponder

Product Specification
Revision 2.1
Confidential

September 1997

PHILIPS

Table of Contents

1. Basic Features of the HITAG System 5

2. Introduction 5

3. Specifications 6

3.1. Transponders / Overview 6
3.2. Electromagnetic Characteristics 6
3.2.1. Magnetic Flux Densities 6
3.2.2. Equivalent Circuit for Data and Energy Transfer 7
3.3. Data Transmission Transponder → Read/Write Device 8
3.3.1. Coding 8
3.3.2. Modulation 9
3.4. Data Transmission Read/Write Device → Transponder 10
3.4.1. Coding 10
3.4.2. Modulation 12
3.5. Switching the transmission direction 13

4. Standard Protocol Modes and Command Set 14

4.1. General Comments 14
4.2. Anticollision Mode 14
4.2.1. Commands 14
4.3. SELECT Mode 16
4.3.1. Command Length 16
4.3.2. Order of a Read Sequence 17
4.3.3. Order of a Write Sequence 18
4.4. HALT Mode 19
4.5. Authentication 20
4.5.1. Authentication Protocol 21

5. Advanced Protocol Modes and Command Set 22

5.1. General Comments 22
5.2. Anticollision Mode 22
5.2.1. Commands 22
5.3. SELECT Mode 24
5.3.1. Command Length 24
5.3.2. Order of a Read Sequence 25
5.3.3. Order of a Write Sequence 26
5.4. HALT Mode 27
5.5. Authentication 28
5.5.1. Authentication Protocol 29

6. Transponder Access / Flow Chart 30

7. Memory Map 31

7.1. General Definitions 32
7.1.1. Definition of the Keys 32
7.1.2. Definition of the Logdata 32
7.2. Configuration of the Transponder 33
7.2.1. Organizing the Configuration Page 33

8. Data Integrity / Calculation of CRC 37

8.1. Basic Concept for Data Reliability 37
8.2. Transmission Read/Write Device to Transponder 37
8.2.1. Read Sequence 37
8.2.2. Write Sequence 38
8.3. Transmission Transponder to Read/Write Device 39
8.3.1. Standard Protocol Mode 39
8.3.2. Advanced Protocol Mode 39
8.4. Source Code for CRC-Checksum 40

Definitions

Data sheet status	
Objective specification	This data sheet contains target or goal specifications for product development.
Preliminary specification	This data sheet contains preliminary data; supplementary data may be published later.
Product specification	This data sheet contains final product specifications.
Limiting values	
Limiting values given are in accordance with the Absolute Maximum Rating System (IEC 134). Stress above one or more of the limiting values may cause permanent damage to the device. These are stress ratings only and operation of the device at these or at any other conditions above those given in the Characteristics section of the specification is not implied. Exposure to limiting values for extended periods may affect device reliability.	
Application information	
Where application information is given, it is advisory and does not form part of the specification.	

Life support applications

These products are not designed for use in life support appliances, devices, or systems where malfunction of these products can reasonably be expected to result in personal injury. Philips Semiconductors customers using or selling these products for use in such applications do so on their own risk and agree to fully indemnify Philips Semiconductors for any damages resulting from such improper use or sale.

1. Basic Features of the HITAG System

hitag™ is the name of one of the universal and powerful product lines of our 125 kHz family. The contactless read/write system that works with passive transponders is suitable for various applications. Inductive coupling helps you to achieve big reading ranges and the use of cryptography guarantees highest data security.
Anticollision (AC) Mode, which is used only in long range operation, allows you to handle several transponders that are within the communication field of the antenna at the same time, thus achieving highest operating security and permitting to handle several transponders (TAGs) quickly and simultaneously.
The HITAG product family is used both in the proximity area (operating range up to about 200 mm) and in the long range area (operating range up to about 1000 mm).

HITAG 1 transponders are highly integrated and do not need any external components beside the HITAG 1 TAG ASIC (HT1 ICS30 02x) and one coil. The memory of the transponder has a size of 2 KBit.

2. Introduction

The HITAG 1 ASIC is a flexible and powerful member of our HITAG™ family. Data are transmitted bidirectionally, in half duplex mode, between read/write device and transponder. To achieve a high level of security, data may be transmitted enciphered.

The following chapters describe the transmission protocols of HITAG 1 TAG ASICs with operating modes, course of operation and timing.

The HITAG 1 TAG ASIC provides two protocol modes, Standard and Advanced Protocol Mode.
These modes are not set by configuration, the user has the possibility to choose among the modes by the proper command set.

The differences between the Standard Protocol Mode and the Advanced Protocol Mode are:
The Advanced Protocol Mode works compared to the Standard Protocol Mode with increased number of Startbits and an 8 Bit Cyclic Redundancy Check (CRC) sent by the TAG ASIC in read operations.

3. Specifications

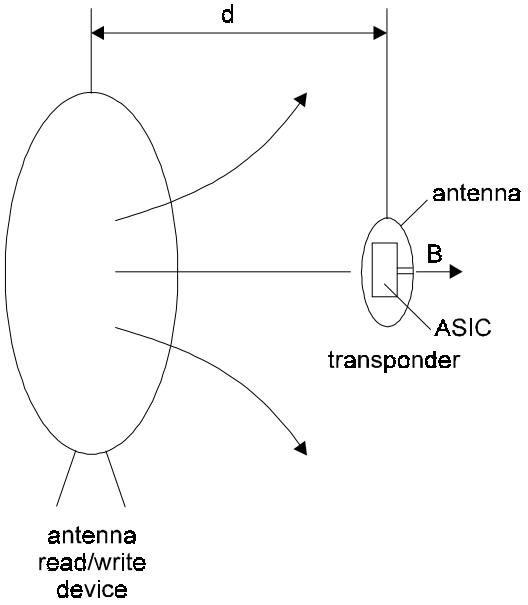
3.1. Transponders / Overview

parameter	
carrier frequency	125 kHz
coding read write	Manchester / AC (anticollision) Pulse Duration
modulation	ASK (amplitude shift keying)
total memory size	2KBit
user memory read/write	224 Byte
read only serial number	32 Bits
data retention	10 years
data security	encryption, authentication, passwords
data integrity	half-duplex handshake, cyclic redundancy check

3.2. Electromagnetic Characteristics

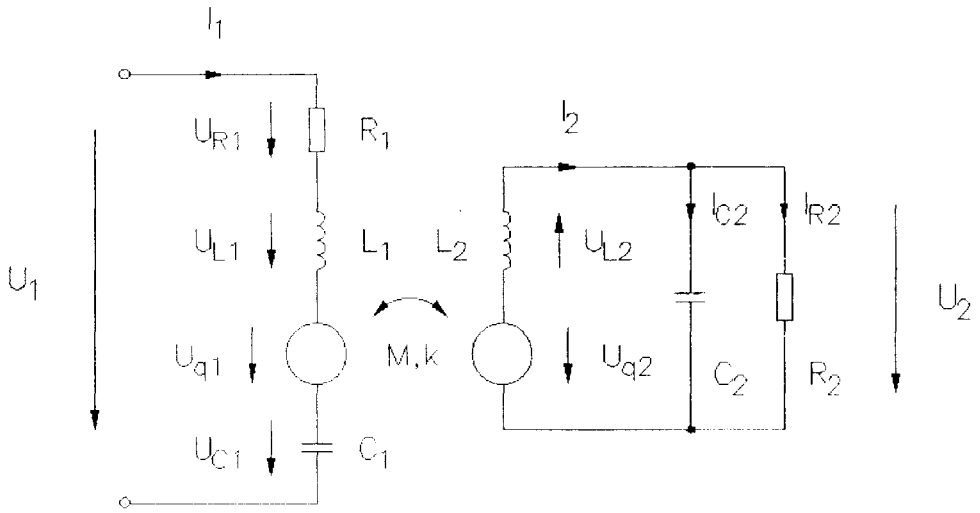
3.2.1. Magnetic Flux Densities

Since magnetic coupling for the data transmission between read/write device (RWD) is used the magnetic field is the most important attribute. The following figure shows the run of the magnetic field lines with the transponder (TAG) placed in the antenna field.



3.2.2. Equivalent Circuit for Data and Energy Transfer

The following drawing shows the model for the transmission channel realised as an inductive coupled circuit. The primary side (L_1) represents the read/write antenna and the secondary side (L_2) the antenna of the transponder.



3.3. Data Transmission Transponder → Read/Write Device

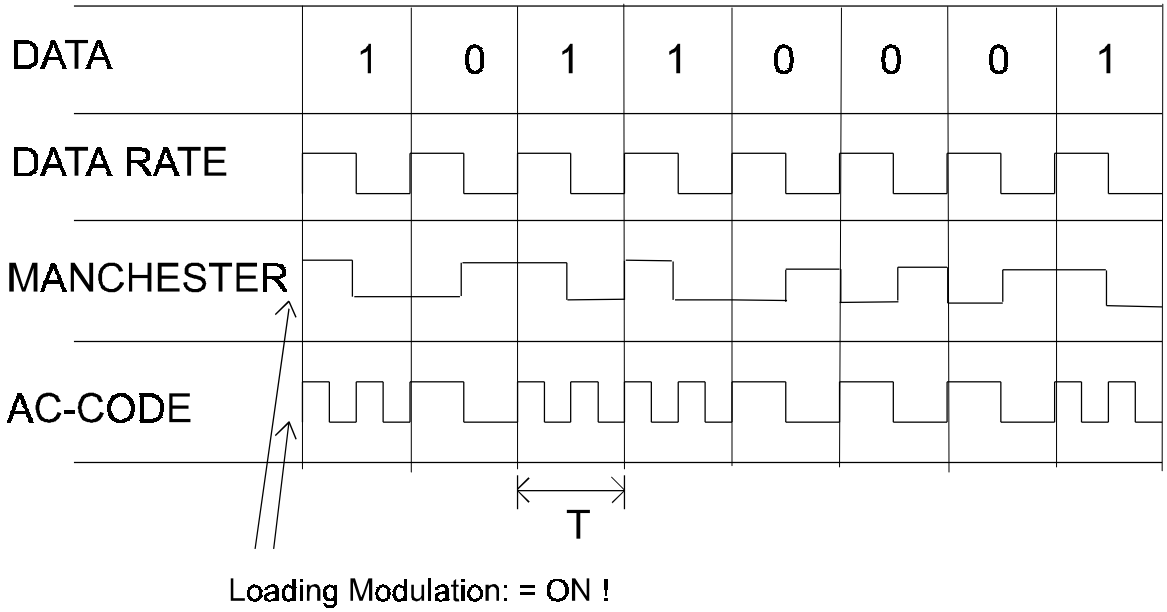
3.3.1. Coding

Absorption modulation is used, when sending data to the read/write device. To force the absorption of the magnetic field, the transponder in principle turns on/off an internal resistor. With the resistor turned on, the physical state is named Modulator ON (loaded) otherwise Modulator OFF (unloaded.)

Two techniques are used for different modes of the transponder (see also chapters "Protocol Modes and Command Set").

Mode	Coding	Bit Length T	Bit rate
Anticollision Mode	AC	64 T_0	2 KBit/s
SELECT Mode	Manchester	32 T_0	4 KBit/s
HALT Mode	Manchester	32 T_0	4 KBit/s

T_0 Carrier period time ($^1/_{125kHz}$ = 8µsec nominal)



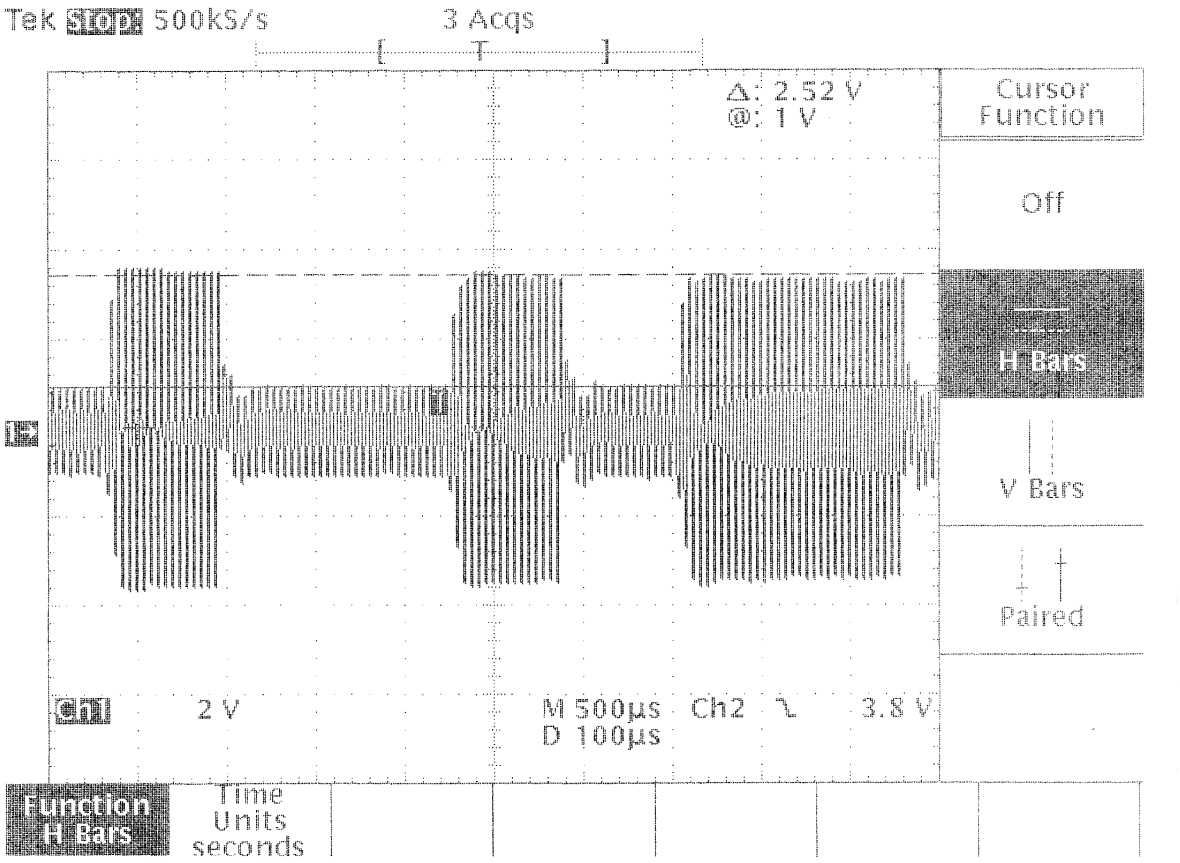
The first bit of the transmitted data always starts with the Modulator ON (loaded) state.

AC-Coding realises the lower baudrate, which is used for anticollision mode. The main part of communication uses the select mode of the transponder.

3.3.2. Modulation

The following figure shows the voltage at the antenna coil of the transponder. It was measured by an additional coil fixed at the transponder.

The minimum modulation ratio depends on the coupling factor of the configuration (read/write antenna, tag antenna size).



3.4. Data Transmission Read/Write Device → Transponder

3.4.1. Coding

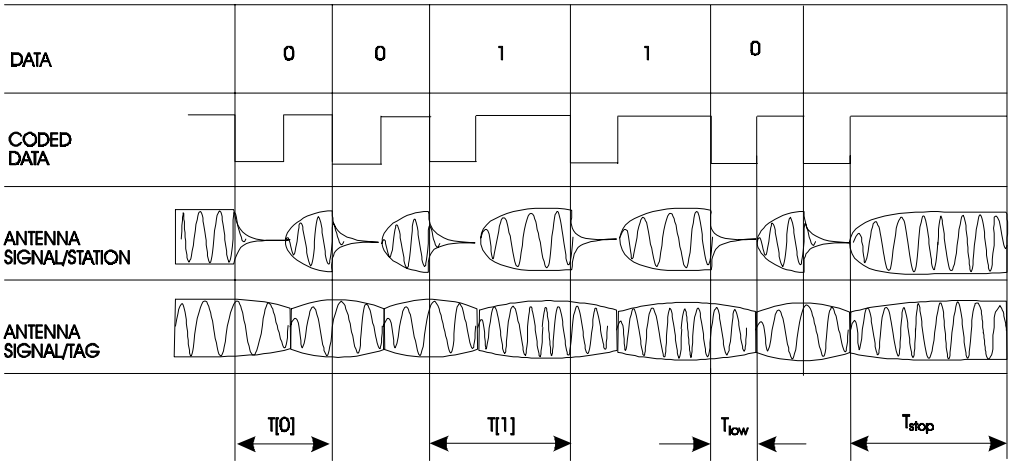
Data are transmitted to the transponder by switching on/off the current through the antenna. When the current is switched off, the physical state is named low field, otherwise high field.

Binary puls length modulation (BPLM) is used to encode the data stream.

All coded data bits and the stop condition start with a low field of length t_{low}.
Afterwards the field is switched on again:

- '0' and '1' can be distinguished by the duration of T[0] and T[1].
- The end of the data transmission is characterized by a stop condition.

The following figure shows the data transmission from the read/write device to the transponder.



Symbol	Description	Duration
t_{low}	low field time	4..10 T_0 *)
T[0]	logic 0 pulse length	18..22 T_0
T[1]	logic 1 pulse length	26..32 T_0
t_{stop}	high field for stop condition	> 36 T_0

*) This application specific value will be within this frame, but has to be optimized for each application depending on antenna current and quality factor!

T_0 Carrier period time ($^1/_{125kHz}$ = 8µsec nominal)

The average Bit rate from the read/write device to transponder therefore is:

$$\text{Bit rate} = \frac{2}{T[0]+T[1]} = 5.2\,\text{KBit / s}$$

Note: The end of each data sequence from read/write device to transponder has to be a stop condition.

Depending on transient and decay times caused by different read/write devices the timing for T[0], T[1] and t_{low} has to be adapted.

The following two examples show the timing for two read/write devices from Philips Semiconductors.

Used timing values with HT RM440 HITAG Proximity Reader Modul are:

Symbol	Description	Duration
t_{low}	low field time	6 T_0
T[0]	logic 0 pulse length	22 T_0
T[1]	logic 1 pulse length	28 T_0

Used timing values with HT RM800 HITAG Long Range Reader Modul are:

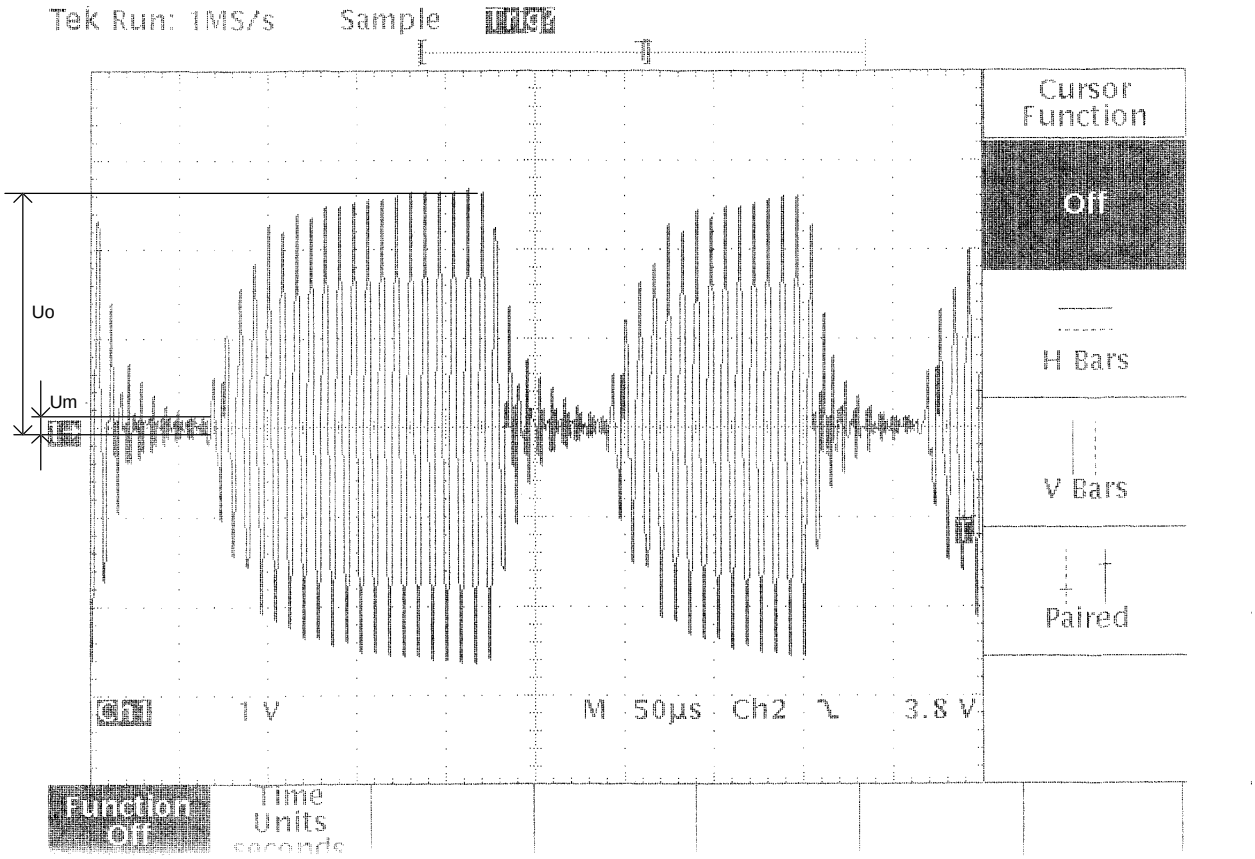
Symbol	Description	Duration
t_{low}	low field time	8 T_0
T[0]	logic 0 pulse length	22 T_0
T[1]	logic 1 pulse length	28 T_0

Please Note: This application specific values have to be optimized for each application !

3.4.2. Modulation

The following figure shows the antenna voltage of the read/write device.

The minimum modulation depends on the quality factor of the antennas (transponder and read/write device) and on the coupling between the antennas.
A recommended value for the quality factor of the read/write device antenna is approx. 40.



3.5. Switching the transmission direction

When switching between receiving and sending, the read/write device has to consider time frames, in which transmission of data is not allowed:

- t_{WAIT1}: When receiving the last bit from the read/write device, the transponder waits before answering.
- t_{WAIT2}: After receiving the last bit from the transponder, the read/write device has to wait before sending data. Data transmitted to the transponder within twait, will not be recognized by the transponder.

Symbol	Description	Duration
t_{WAIT1}	transponder switching from receive to transmit, wait time after end of data	min. 204 T_0...max 213 T_0
t_{WAIT2}	transponder switching from transmit to receive, wait time after end of data	min. 128 T_0 in AC Coding*) min. 90 T_0 in Manchester Coding*)

*) t_{WAIT2} must not exceed 5000 T_0!

4. Standard Protocol Modes and Command Set

4.1. General Comments

The Standard Protocol Mode also allows operation with transponders based on the TAG ASIC HT1 ICS30 0**1**x (transponder type names HT1 DCxx S30/x/**N**).

(HT1 ICS30 0**1**x is the predecessor version of the TAG ASIC HT1 ICS30 0**2**x.)

The response time of the transponder starts with the detection of the last pause of the carrier signal in a read/write device (RWD) command.

Note : The grey fields in the timing information are defined by digital processes and are therefore fixed.

T_0 Carrier period time ($^1/_{125kHz}$ = 8µsec nominal).

4.2. Anticollision Mode

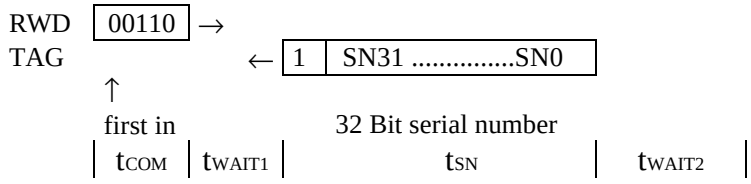
The command to read the serial numbers of all transponders (TAGs) presently located in the field of the read/write antenna uses Anticollision Mode (AC-Mode). As the serial number (SN) is 32 Bits long, theoretically up to 2^{32} TAGs can be in this mode.

Use the SELECT command to exit AC-Mode.

4.2.1. Commands

4.2.1.1. SET_CC

After transmitting this command from the read/write device, all transponders presently located in the field of the read/write antenna respond with One (Startbit) followed by the corresponding 32 Bit serial number (SN). The response of the transponder is transmitted in Anticollision Code.

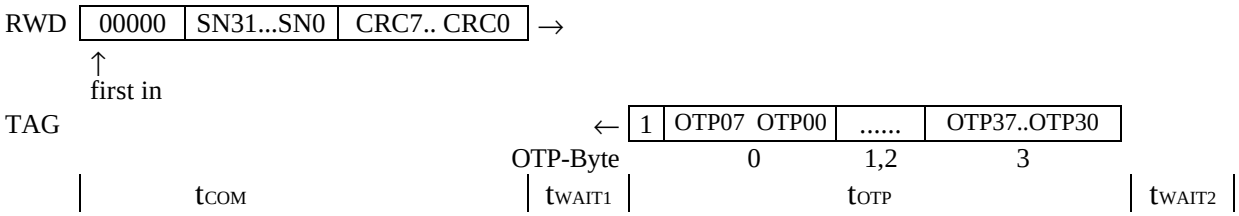


	MIN	TYP	MAX	Unit
t_{COM}	119.5	122	124.5	T_0
t_{WAIT1}	204	208.5	213	T_0
t_{SN}		2112		T_0
t_{WAIT2}	128		5000	T_0
total		2570		T_0

RWD ... Read/Write Device
TAG ... Transponder

4.2.1.2. SELECT

The command SELECT consists of 5 Zero-Bits followed by the determined 32 Bit serial number and an 8 Bit Cyclic Redundancy Check (CRC). The selected transponder then responds with One (Startbit) followed by 32 Bits representing the configuration page. The transponder response is not carried out in Anticollision Code (AC) but already in Manchester Code.



	MIN	TYP	MAX	Unit
t_{COM} 1)		1110		T_0
t_{WAIT1}	204	208.5	213	T_0
t_{OTP}		1056		T_0
t_{WAIT2}	96		5000	T_0
total		2500		T_0

1) depends on the data sent to the TAG
(intervals for logic 0 and logic 1 are different)

4.3. SELECT Mode

You use SELECT Mode to read data from and write data on a transponder. In this mode you can work either with cryptography (secret) or without (plain) (see Chapter 4.4, Authentication).
A transponder can be read or written or muted after processing.

Command set-up in SELECT_MODE

COMMAND CMD3 .....CMD0	ADDRESS	CRC

COMMAND: Command (4 Bits)

ADDRESS: Address (8 Bits, MSB first), indicates the start of a page or block respectively.
A7 and A6 must be 0 (highest page number is 63, see also chapter 7)

CRC: Check byte (8 Bits, MSB first)

The following commands are supported:

COMMAND	**CODE CMD 3 2 1 0**	**Read**	**Write**	**Block CMD**	**Encrypted**	**Plain**	**Notes**
WRPPAGE	1 0 0 0	no	yes	no	no	yes	Writes a plain page
WRPBLK	1 0 0 1	no	yes	yes	no	yes	Writes a plain block
WRCPAGE	1 0 1 0	no	yes	no	yes	no	Writes a crypto page
WRCBLK	1 0 1 1	no	yes	yes	yes	no	Writes a crypto block
RDPPAGE	1 1 0 0	yes	no	no	no	yes	Reads a plain page
RDPBLK	1 1 0 1	yes	no	yes	no	yes	Reads a plain block
RDCPAGE	1 1 1 0	yes	no	no	yes	no	Reads a crypto page
RDCBLK	1 1 1 1	yes	no	yes	yes	no	Reads a crypto block
HALT	0 1 1 1	no	no	no			Turns into HALT Mode

↑
First in

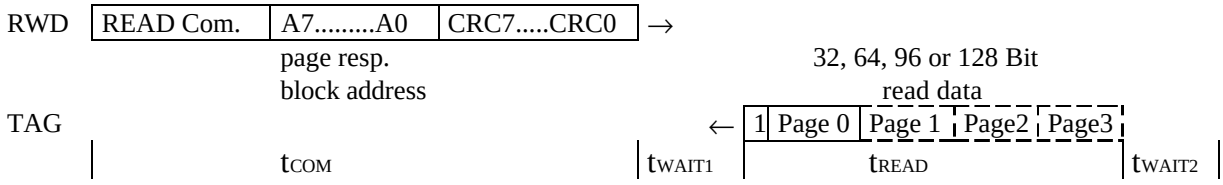
4.3.1. Command Length

Length [Bits] = L {COMMAND} + L {ADDRESS} + L {CRC} =
4 + 8 + 8 = 20 Bits

So the number of Bits for a command is always 20, no matter which command.

4.3.2. Order of a Read Sequence

After transmitting a READ command, the address and the 8 Bit Cyclic Redundancy Check (CRC), the transponder responds with One (Startbit) and 32, 64, 96 or 128 Bits data. It depends on whether the command was a READ Page or a READ Block command. If you do not indicate the beginning of a block but a page within this block as the address for a READ Block command, then all pages starting from this address to the end of the block will be sent to the read/write device.

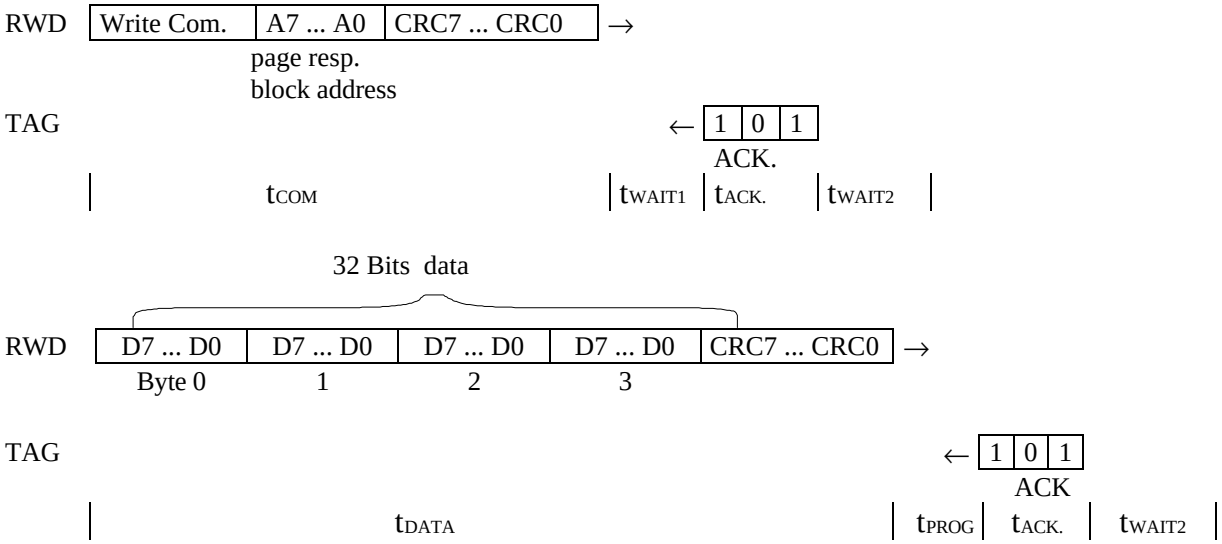


	MIN	TYP	MAX	Unit
t_{COM} 1)	440	500	550	T_0
t_{WAIT1}	204	208.5	213	T_0
t_{READ} 2)	1056		4128	T_0
t_{WAIT2}	96		5000	T_0
total 3)		1857		T_0
total 4)		4929		T_0

1) depends on the data (read command, address, CRC)
2) depends on page- or block access
3) Page Access
4) Block Access

4.3.3. Order of a Write Sequence

The EEPROM is organised byte by byte. However, the protocol read/write device to transponder supports only access to a page or a complete block. To avoid temporary storage of a block in the transponder (before programming takes place) data is transmitted to the transponder only page by page. Every word is protected by a check byte and an acknowledgement signal from the transponder confirms correct programming. This acknowledgement is always done in plain form.



With a Write Page command the last part of this protocol is executed only once. With a Write Block command this part is executed one to four times, depending on whether the address indicates the beginning of a block or the beginning of one of the three remaining pages within that block.

	MIN	TYP	MAX	Unit
t_{COM} 1)	440	500	550	T_0
t_{WAIT1}	204	208.5	213	T_0
$t_{ACK.}$		96		T_0
t_{WAIT2}	96		5000	T_0
t_{DATA} 2)		1000		T_0
t_{PROG}	716	721	726 3)	T_0
total 4)		2800		T_0
total 5)		8550		T_0

1) depends on the data (write command, address, CRC)
2) depends on page- or block access and on the data
3) for flexibility reasons (perhaps the use of future EEPROM blocks with different timing) we recommend to calculate with t_{PROG} of max. 1250 T_0.
4) Page Access
5) Block Access

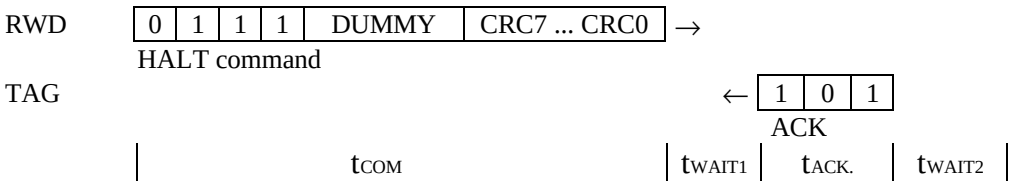
Attention: For transponders based on the TAG ASIC HT1 ICS30 0*1*x t_{PROG} must be max. 1250T_0 !!

4.4. HALT Mode

The HALT Mode is used to disable a selected transponder remaining in the reading area of the read/write device.
Multitag operations handled by the long range reader use this mode. This mode may be a useful feature for proximity applications, too. By muting a selected transponder (HALT Mode) another transponder, that is to be found in the communication field of the antenna, can be recognized.

A transponder, once turned to HALT Mode, can only be enabled by executing a *power on reset*. This means either the power supply of the transponder (magnetic field) must be interrupted for about 10 ms or the transponder must be moved out of the antenna field.

This command may be ciphered or not, depending on the current operating mode of the transponder (plain or ciphered).



	MIN	TYP	MAX	Unit
t_{COM}	448	500	564	T_0
t_{WAIT1}	204	208.5	213	T_0
$t_{ACK.}$		96		T_0
t_{WAIT2}	96		5000	T_0
total		900		T_0

Dummy
This parameter must be sent for command length reasons only. CRC must be valid although the transponder does not process this data. As the HALT command is a plain command, the dummy data must be a valid address pointing to a plain area (greater than or equal to 00100000, A7 and A6 must be 0 too).

4.5. Authentication

In order to be able to operate HITAG 1 transponders in Encrypted Mode Keys and Logdata of RWD and TAG have to be identically. You have to process an authentication protocol first. The crypto blocks on the read/write device and on the transponder respectively get the same start value and are thus able to work synchronously.

The command WRCPAGE is also used to start the authentication process, followed by some 8 Bit information (see table below) indicating which key with the respective logdata the authentication uses, and an 8 Bit CRC. The transponder returns an acknowledgement signal.
After sending a 32 Bit random number to the transponder, the start value for the crypto block is defined.

Up to this point the protocol uses plain text. From now on both crypto blocks have the same start value so the protocol continues in encrypted form.

The transponder responds to the random number with the Startbit and the 32 Bit Logdata 0A or 0B, then the read/write device sends 32 Bit Logdata 1A or 1B to the transponder. These are acknowledged by the transponder.

The Authentication Protocol contains the information, which of the two sets of Key and Logdata (A or B) are used (see chapter 4.4.1).

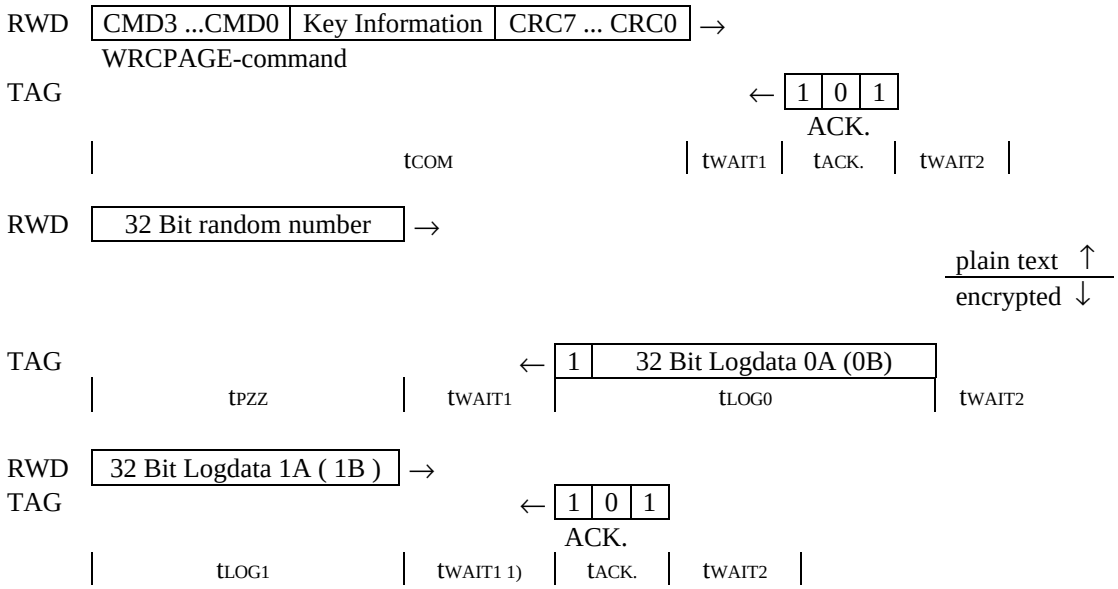
The following table shows the connection between Key Information and set of Key and Logdata:

Key Information	Logdata TAG --> Read/Write Device	Logdata Read/Write Device -->TAG
0 0 0 0 0 0 0 0	Logdata 0A	Logdata 1A
0 0 0 0 0 0 1 0	Logdata 0B	Logdata 1B

↑
First in

The RWD has to use the according Key for encoding and decoding of the data.

4.5.1. Authentication Protocol



1) Attention: For transponders based on the TAG ASIC HT1 ICS30 0*1*x this t_{WAIT1} only is 72 ± ½ T_0.

	MIN	TYP	MAX	Unit
t_{COM}	470	473	476	T_0
t_{WAIT1}	204	208.5	213	T_0
$t_{ACK.}$		96		T_0
t_{WAIT2}	96		5000	T_0
t_{PZZ}	704	800	896	T_0
t_{LOG0}		1056		T_0
t_{LOG1}	704	800	896	T_0
total		4220		T_0

After start-up of the authentication process the protocol for the selected transponder runs in Encrypted Mode. However, acknowledgement is sent in plain text.

To return to Plain Text Mode you have to send a plain text command. As the transponder is still in Encrypted Mode this plain text command has to be sent in encrypted form. If you use a READ command the answer is already sent in plain text.

5. Advanced Protocol Modes and Command Set

5.1. General Comments

The new Advanced Protocol Mode works compared to the Standard Protocol Mode with increased number of Startbits and an 8 Bit CRC sent by the ASIC for read operations.

This communication protocol is **not supported** by transponders based on TAG ASIC **HT1 ICS30 0*1*x**.

The response time of the transponder starts with the detection of the last pause of the carrier signal in an RWD command.

Note : The grey fields in the timing information are defined by digital processes and are therefore fixed.

T_0 Carrier period time ($^1/_{125kHz}$ = 8µsec nominal).

5.2. Anticollision Mode

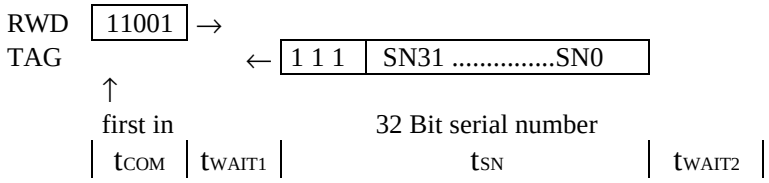
The command to read the serial numbers of all transponders (TAGs) presently located in the field of the read/write antenna uses Anticollision Mode (AC-Mode). As the serial number is 32 Bits long, theoretically up to 2^{32} TAGs can be in this mode.

Use the SELECT command to exit AC-Mode.

5.2.1. Commands

5.2.1.1. SET_CCNEW

After transmitting this command from the read/write device, all transponders presently located in the field of the read/write antenna respond with three Startbits followed by the corresponding 32 Bit serial number. The response of the transponder is transmitted in Anticollision Code.



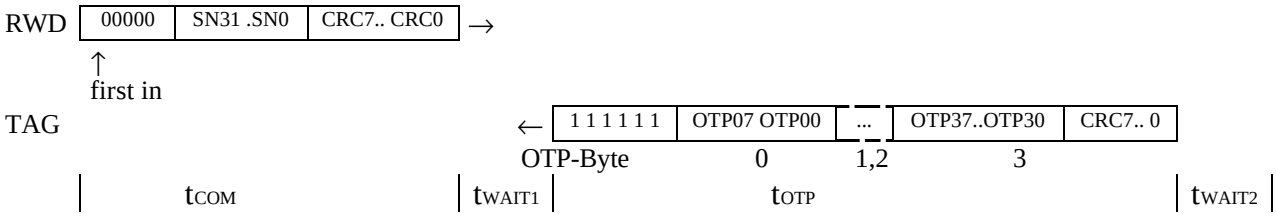
	MIN	TYP	MAX	Unit
t_{COM}	125	128	131	T_0
t_{WAIT1}	204	208.5	213	T_0
t_{SN}		2240		T_0
t_{WAIT2}	128		5000	T_0
total		2635		T_0

The command SET_CCNEW can be repeated as long as the transponder is in AC-Mode.

PLEASE NOTE: If the command SET_CCNEW is transmitted once the transponder stays in the Advanced Protocol Mode, even if a SET_CC command (Standard Protocol Mode) is transmitted. Only a *power on reset* of the TAG ASIC (power supply of the TAG must be interrupted for about 10ms) is able to reset this Advanced Protocol Mode.

5.2.1.2. SELECT

The command SELECT consists of 5 Zero-Bits followed by the determined 32 Bit serial number and an 8 Bit CRC. The selected transponder then responds with the start sequence (6 ones) followed by 32 Bits representing the configuration page and 8 Bits CRC. The transponder response is not carried out in Anticollision Code but already in Manchester Code.



	MIN	TYP	MAX	Unit
t_{COM} 1)	967	1125	1253	T_0
t_{WAIT1}	204	208.5	213	T_0
t_{OTP}		1472		T_0
t_{WAIT2}	96		5000	T_0
total		2900		T_0

1) depends on the data sent to the TAG
(intervals for logic 0 and logic 1 are different)

5.3. SELECT Mode

You use SELECT Mode to read data from and write data on a transponder. In this mode you can work either with cryptography (secret) or without (plain) (see Chapter 5.4, Authentication).
A transponder can be read or written or muted after processing.

Command set-up in SELECT_MODE

COMMAND CMD3 .....CMD0	ADDRESS	CRC

COMMAND: Command (4 Bits)

ADDRESS: Address (8 Bits, MSB first), indicates the start of a page or block respectively.
A7 and A6 must be 0 (highest page number is 63, see also chapter 7).

CRC: Check byte (8 Bits, MSB first)

The following commands are supported:

COMMAND	CODE CMD 3 2 1 0	Read	Write	Block CMD	Encrypted	Plain	Notes
WRPPAGE	1 0 0 0	no	yes	no	no	yes	Writes a page
WRPBLK	1 0 0 1	no	yes	yes	no	yes	Writes a block
WRCPAGE	1 0 1 0	no	yes	no	yes	no	Writes a page
WRCBLK	1 0 1 1	no	yes	yes	yes	no	Writes a block
RDPPAGE	1 1 0 0	yes	no	no	no	yes	Reads a page
RDPBLK	1 1 0 1	yes	no	yes	no	yes	Reads a block
RDCPAGE	1 1 1 0	yes	no	no	yes	no	Reads a page
RDCBLK	1 1 1 1	yes	no	yes	yes	no	Reads a block
HALT	0 1 1 1	no	no	no			Turns into HALT Mode

↑
First in

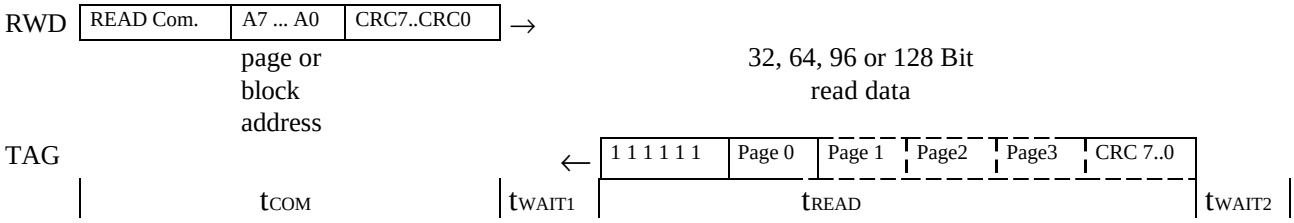
5.3.1. Command Length

Length [Bits] = L {COMMAND} + L {ADDRESS} + L {CRC} =
4 + 8 + 8 = 20 Bits

So the number of Bits for a command is always 20, no matter which command.

5.3.2. Order of a Read Sequence

After transmitting a READ command, the address and the 8 Bit CRC, the transponder responds with the startsequence (6 ones) and 32, 64, 96 or 128 Bits data, depending on whether the command was a READ Page or a READ Block command. If you do not indicate the beginning of a block but a page within this block as the address for a READ Block command, then all pages starting from this address to the end of the block will be sent to the read/write device.

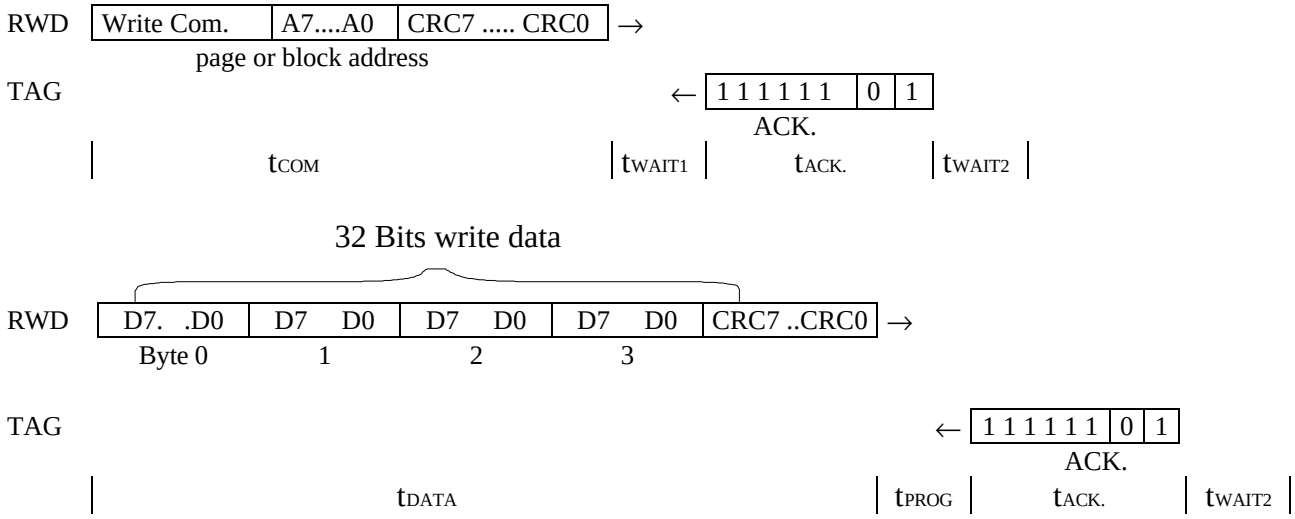


	MIN	TYP	MAX	Unit
t_{COM} 1)	442	500	564	T_0
t_{WAIT1}	204	208.5	213	T_0
t_{READ} 2)	1472		4544	T_0
t_{WAIT2}	96		5000	T_0
total 3)		2280		T_0
total 4)		5346		T_0

1) depends on the data (read command, address, CRC)
2) depends on page- or block access
3) Page Access
4) Block Access

5.3.3. Order of a Write Sequence

The EEPROM is organised byte by byte. However, the protocol read/write device to transponder supports only access to a page or a complete block. To avoid temporary storage of a block in the transponder (before programming takes place) data is transmitted to the transponder only page by page. Every word is protected by a check byte and an acknowledgement signal from the transponder confirms correct programming. This acknowledgement is always done in plain form.



With a Write Page command the last part of this protocol is executed only once. With a Write Block command this part is executed one to four times, depending on whether the address indicates the beginning of a block or the beginning of one of the three remaining pages within that block.

	MIN	TYP	MAX	Unit
t_{COM} 1)	442	500	564	T_0
t_{WAIT1}	204	208.5	213	T_0
$t_{ACK.}$		256		T_0
t_{WAIT2}	96		5000	T_0
t_{DATA} 2)		1000		T_0
t_{PROG}	716	721	726 3)	T_0
total 4)		3125		T_0
total 5)		9330		T_0

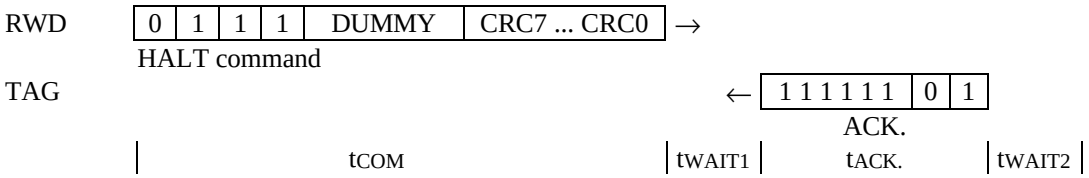
1) depends on the data (write command, address, CRC)
2) depends on page- or block access and on the data
3) for flexibility reasons (perhaps the use of future EEPROM blocks with different timing) we recommend to calculate with t_{PROG} of max. 1250 T_0
4) Page Access
5) Block Access

5.4. HALT Mode

The HALT Mode is used to disable a selected transponder remaining in the reading area of the read/write device.
Multitag operations handled by the long range reader use this mode. This mode may be a useful feature for proximity applications, too. By muting a selected transponder (HALT Mode) another transponder, that is to be found in the communication field of the antenna, can be recognized.

A transponder, once turned to HALT Mode, can only be enabled by executing a *power on reset*. This means either the power supply of the transponder must be interrupted for about 10 ms or the transponder must be moved out of the antenna field.

This command may be ciphered or not, depending on the current operating mode of the transponder (plain or ciphered).



	MIN	TYP	MAX	Unit
t_{COM}	448	500	564	T_0
t_{WAIT1}	204	208.5	213	T_0
$t_{ACK.}$		256		T_0
t_{WAIT2}	96		5000	T_0
total		1060		T_0

Dummy
This parameter must be sent for command length reasons only. CRC must be valid although the transponder does not process this data. As the HALT command is a plain command, the dummy data must be a valid address pointing to a plain area (greater than or equal to 00100000, A7 and A6 must be 0 too).

5.5. Authentication

In order to be able to operate HITAG 1 transponders in Encrypted Mode Keys and Logdata of RWD and TAG have to be identically. You have to process an authentication protocol first. The crypto blocks on the read/write device and on the transponder respectively get the same start value and are thus able to work synchronously.

The command WRCPAGE is also used to start the authentication process, followed by some 8 Bit information (see table below) indicating which key with the respective logdata the authentication uses, and an 8 Bit CRC. The transponder returns an acknowledgement signal.
After sending a 32 Bit random number to the transponder, the start value for the crypto block is defined.

Up to this point the protocol uses plain text. From now on both crypto blocks have the same start value so the protocol continues in encrypted form.

The transponder responds to the random number with the Startbit and the 32 Bit Logdata 0A or 0B, then the read/write device sends 32 Bit Logdata 1A or 1B to the transponder. These are acknowledged by the transponder.

The Authentication Protocol contains the information, which of the two sets of Key and Logdata (A or B) are used (see chapter 5.4.1).

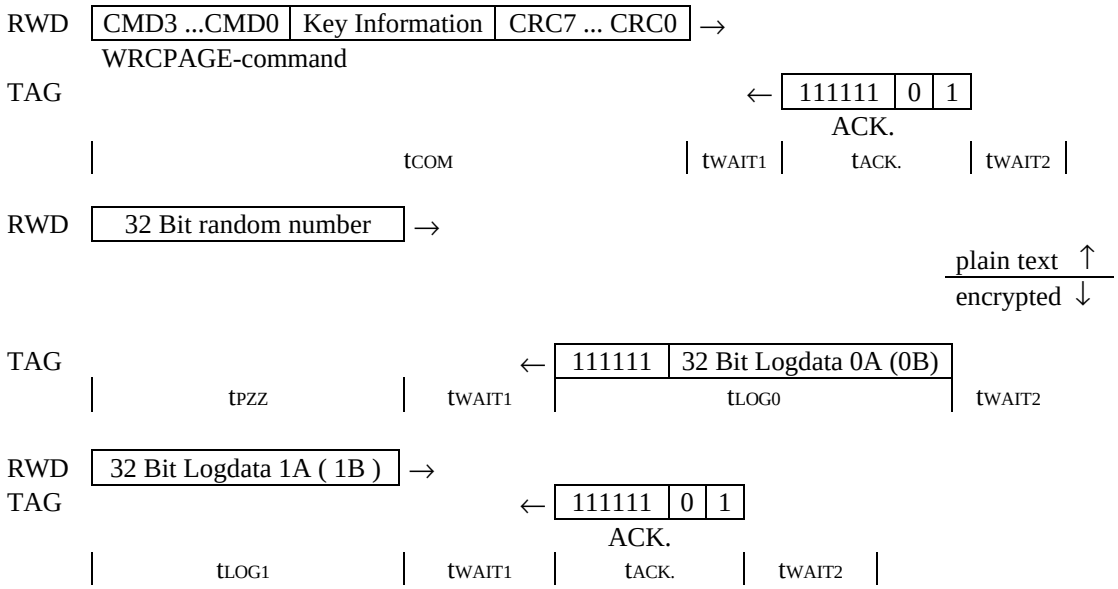
The following table shows the connection between Key Information and set of Key and Logdata:

Key Information	Logdata TAG --> Read/Write Device	Logdata Read/Write Device -->TAG
0 0 0 0 0 0 0 0	Logdata 0A	Logdata 1A
0 0 0 0 0 0 1 0	Logdata 0B	Logdata 1B

↑
First in

The RWD has to use the according Key for encoding and decoding of the data.

5.5.1. Authentication Protocol

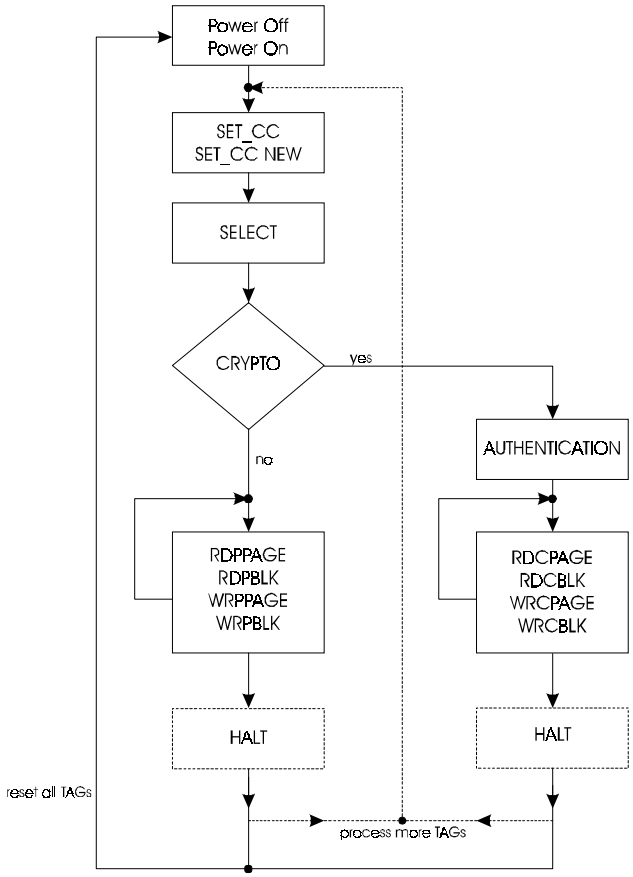


	MIN	TYP	MAX	Unit
tCOM	470	473	476	T_0
tWAIT1	204	208.5	213	T_0
tACK.		256		T_0
tWAIT2	96		5000	T_0
tPZZ	704	800	896	T_0
tLOG0		1216		T_0
tLOG1	704	800	896	T_0
total		4710		T_0

After start-up of the authentication process the protocol for the selected transponder runs in Encrypted Mode. However, acknowledgement is sent in plain text.

To return to Plain Text Mode you have to send a plain text command. As the transponder is still in Encrypted Mode this plain text command has to be sent in encrypted form. If you use a READ command the answer is already sent in plain text.

6. Transponder Access / Flow Chart



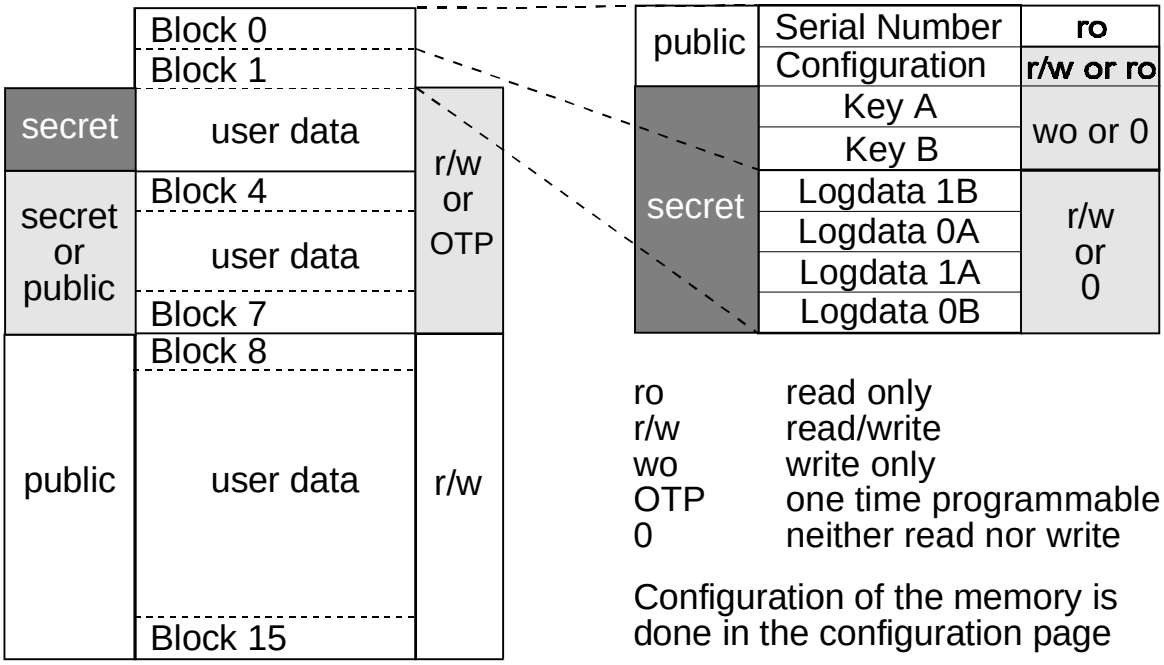
POWER OFF	...	The read/write device turns off the 125 kHz transmitter to put the transponder in its initial (reset) state
POWER ON	...	The read/write device activates the 125 kHz transmitter to supply the transponder with energy (TAG power up time ~ 3 ms)
SET_CC, SET_CC NEW	...	After receiving the SET_CC (SET_CC NEW) command the transponder responds with its serial number
SELECT	...	The transponder is selected by its serial number and responds with its configuration (configuration page)
AUTHENTICATION	...	By carrying out mutual authentication the Encrypted Mode for transmission is entered
HALT	...	The transponder is deactivated (not necessary for single transponder operation)

7. Memory Map

The 2 KBit memory area in the EEPROM of the HITAG 1 TAG ASIC is divided into 16 blocks. Each block comprises 4 pages with 4 bytes (at 8 Bits) each. A page is the smallest access unit.

Addressing is done page by page (Page 0 .. 63) and access is gained either page by page or block by block entering the respective start address. In case of block read/write the transponder is processed from the start address to the end of the block.

Block access is only available for Blocks 2-15, page access is available for Pages 0-63.



Areas (or settings) with light dark background may be configured by the OEM client using the Configuration Page (Page 1).

Memory locations marked with "secret" can only be accessed after a mutual authentication. An enciphered data communication is used in that area.
Memory locations marked with "public" can be accessed without mutual authentication, no encryption is used.

Block 0 includes the unique serial number (programmed during the production process), the Configuration Page (configuration of the memory area) and the keys, Block 1 includes the logdata.

7.1. General Definitions

Secret / Public: Access to an address in the secret area of the transponder is only possible using cryptography and mutual authentication. Access to the plain memory area is only possible without cryptography (plain).

Block 0 defines the unique serial number (programmed during the production), the configuration page (configuration of the memory area) and the keys, Block 1 defines the logdata.

Blocks 4 to 7 can be used either as secret or public areas (configurable), and Blocks 2 to 7 either as read/write or read only areas (configurable). You can also modify keys and logdata and prevent them from being accessed.

Finally the configuration page itself can be set to read only.

It is extremely important to be particularly careful when using the configuration page (it can be set to read only once!), keys and logdata as an error can result in loss of access to the secret area on the transponder.

Attention: Changing of the configuration page (page 1), Keys and Logdata must be done in secure environment. The transponder must not be moved out of the communication field of the antenna during programming! We recommend to put the transponder close to the antenna (zero-distance) and not to remove it during programming.

7.1.1. Definition of the Keys

Keys are cryptographic codes, which determine data encryption during data transfer between the read/write device and transponder.

The keys are predefined by Philips Semiconductors by means of defined Transport Keys (both keys show the same Bitmap). They can be written to, which means that they can be changed.

The predefined values are: Key A: 0x00000000, Key B: 0x00000000.

7.1.2. Definition of the Logdata

Logdata represent "passwords" needed to gain access to secret areas on the transponder. Every cryptographic key (Key A and Key B) includes a pair of logdata. This logdata pair has to be identical both on the transponder and the read/write device.

ad Key A:	Logdata 0 A	"Password" that the transponder sends to the read/write device and which is verified by the latter.
	Logdata 1 A	"Password" that the read/write device sends to the transponder and which is checked for identity by the latter.

ad Key B:	Logdata 0 B and	
	Logdata 1 B	analogous to Key A

The logdata are also predefined by Philips Semiconductors using defined Transport Logdata (all logdata show the same Bitmap). They can be read and written. Logdata 0A and 1A, as well as Logdata 0B and 1B do not have to show the same values, but Logdata 0A/B and 1A/B have to be identical on the read/write device and on the transponder !

The predefined values are: Logdata 0A: 0x00000000, Logdata 0B: 0x00000000.
Logdata 1A: 0x00000000, Logdata 1B: 0x00000000.

Attention: Keys and Logdata only can be changed if the Transport Key and the Transport Logdata are known!

7.2. Configuration of the Transponder

You have the possibility to configure parts of the memory area on the transponder according to your needs. You realise this configuration in the configuration page (page 1 of the TAG memory). This is where you also define whether keys and logdata (personalization of the transponders) can be changed or not.

7.2.1. Organizing the Configuration Page

The configuration page consists of 4 bytes, the first two of which are fixed (in the following called One Time Programmable bytes), the other two bytes are still free.

The Bitmaps in One Time Programmable (OTP) Bytes 0 and 1 determine the configuration of the memory. They define which area is secret or public, r/w, ro, wo or neither read nor write.

You can allocate and write the OTP bytes freely until the configuration page is locked (OTP Byte 1, Bit 4 is set to ”0”).
After this these bytes are read only bytes and the configuration of the transponder cannot be changed any more.

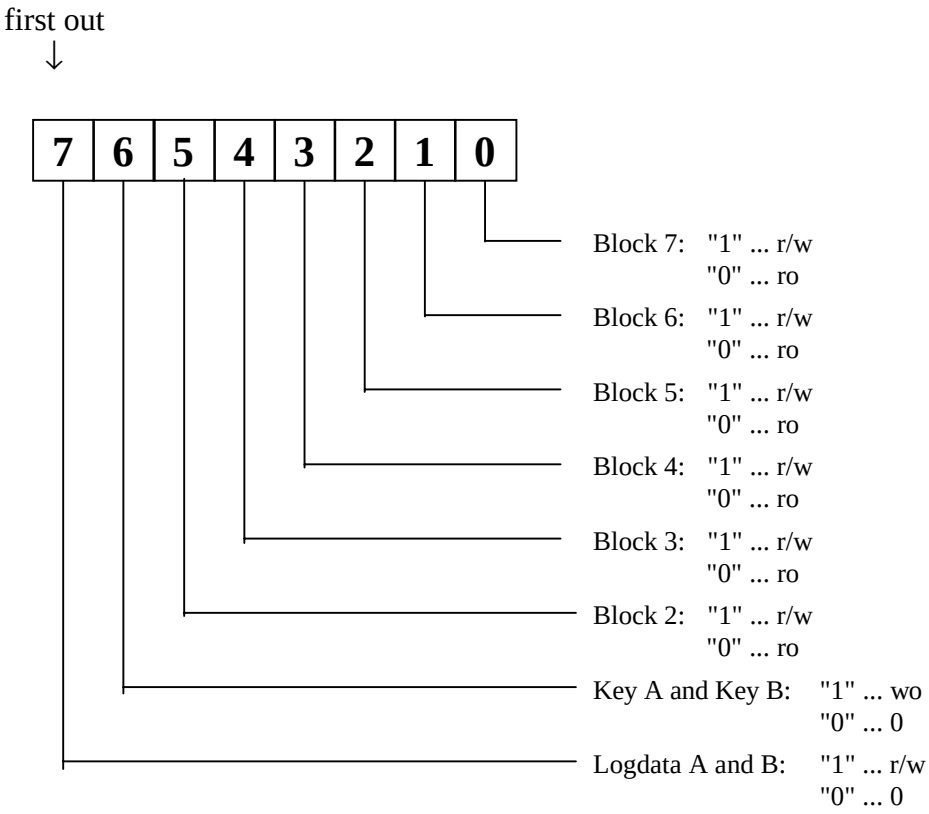
Attention: Once set to ro a configuration page cannot be changed back to r/w again (transponder is hardware protected)!

Configuration Bytes 2 and 3: These two bytes, too, are set to read only by the OEM Lock Bit (Configuration Byte 1 / Bit 4 = ”0”). Considering that fact you can use these two bytes freely. They will not affect memory configuration.

Explanations of abbreviations used:

r/w	read and write
ro	read only
wo	write only
0	neither read nor write

7.2.1.1. Configuration Byte 0



Configuration Byte 0 / Bit 7:

Bit 7 = ‘1’: Logdata can be read and written to.
Bit 7 = ‘0’: Logdata cannot be accessed.

This Bit can be set or reset until Bit 4 of Configuration Byte 1 is set to ‘0’.

Configuration Byte 0 / Bit 6:

Bit 6 = ‘1’: Keys can only be written to.
Bit 6 = ‘0’: Keys cannot be accessed.

This Bit can be set or reset until Bit 4 of Configuration Byte 1 is set to ‘0’.

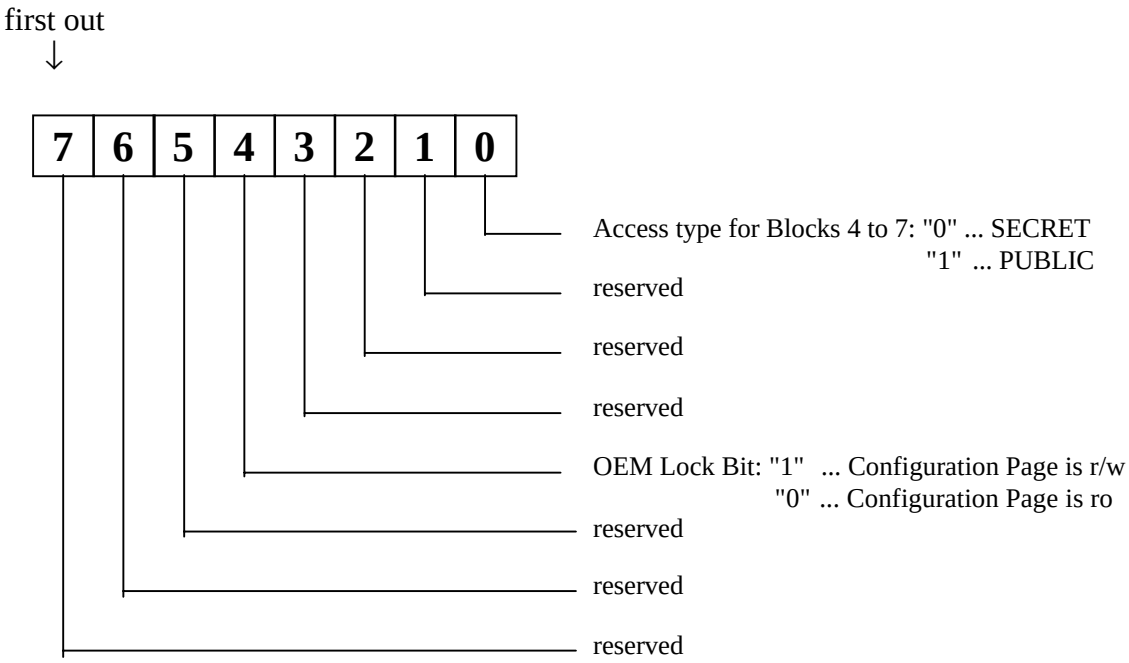
Configuration Byte 0 / Bits 0 ... 5:

If one of these Configuration Bits is ‘1’, the corresponding block of the transponder can be read and written.
If the Bit is set to ‘0’, the corresponding block can only be read.

Within one block the configuration is always identical, that means either all 4 pages are read/write or all of them are read only.

These Bits can be set or reset until Bit 4 of Configuration Byte 1 is set to ‘0’.

7.2.1.2. Configuration Byte 1



Configuration Byte 1 / Bits 5 ... 7:

These three Bits are reserved.

ATTENTION: When writing a new value to Configuration Byte 1, Bit positions marked as "reserved" must not be altered. To meet that condition read the current Configuration Byte 1 value and mask in your new values for Bit positions you are allowed to change.

Configuration Byte 1 / Bit 4:

Bit 4 = '1': Configuration Page can be read and written to.
Bit 4 = '0': Configuration Page can only be read. This process is irreversible !

ATTENTION: Do not set Bit 4 of Configuration Byte 1 to '0' before having written the final data into the Configuration Page of the transponder.

Configuration Byte 1 / Bits 1 ... 3:

These three Bits are reserved.

ATTENTION: When writing a new value to Configuration Byte 1, Bit positions marked as "reserved" must not be altered. To meet that condition read the current Configuration Byte 1 value and mask in your new values for Bit positions you are allowed to change.

Configuration Byte 1 / Bit 0:

Bit 0 = '0': Access type for Blocks 4 to 7 is SECRET.
Bit 0 = '1': Access type for Blocks 4 to 7 is PUBLIC.

This Bit can be set or reset until Bit 4 of Configuration Byte 1 is set to '0'.

7.2.1.3. Configuration of Delivered HITAG 1 Transponders

HITAG 1 transponders are delivered with the following configuration by Philips Semiconductors:

Unique Serial Number:

Serial Number:	Read Only	-	fixed

Configuration Byte 0:

Logdata:	'1' = r/w	-	can be changed
Key A, Key B:	'1' = wo	-	can be changed
Blocks 2 - 7:	'1' = r/w	-	can be changed

Configuration Byte 1:

OEM Lock Bit:	'1' = Configuration Page is r/w	-	can be changed
Blocks 4 - 7:	'1' = public	-	can be changed

Value for Transport Keys, Transport Logdata:

`0x00000000`

8. Data Integrity / Calculation of CRC

8.1. Basic Concept for Data Reliability

The following explanations show the features of the HITAG system to protect read and write access to transponders from undetected errors. It is sufficient to investigate the unciphered read and write operations because the stream cipher does not effect the data integrity of transmission.

8.2. Transmission Read/Write Device to Transponder

Every data stream (commands, addresses, user data) sent to the transponder includes an 8 Bit CRC calculated by the read/write device. The data stream is first checked for data errors by the TAG ASIC and then executed.

The CRC is formed over commands and addresses or the plain data respectively and in case of Encrypted Mode it is also encrypted.

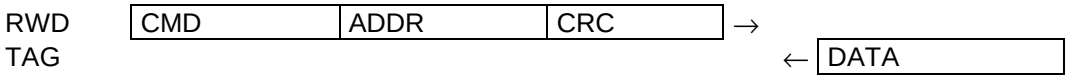
The generator polynomial for the CRC reads:

$$u^8 + u^4 + u^3 + u^2 + 1 \quad = \quad 0x1D$$

and the CRC preassignment is 0xFF

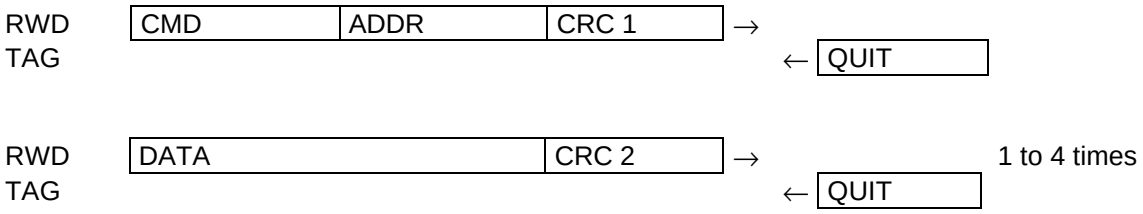
For better understanding the protocols for reading and writing are outlined.

8.2.1. Read Sequence



TAG ... transponder
RWD ... read/write device
CMD ... command, 4 Bits (read page, read block, read page ciphered, read block ciphered)
ADDR ... address, 8 Bits (page or block address for page or block read)
CRC ... cyclic redundancy check, 8 Bits (check sum of CMD and ADDR)
DATA ... read data, 32 Bits to 128 Bits (one to four pages for page or block read)

8.2.2. Write Sequence



CMD ... command, 4 Bits (write page, write block, write page ciphered, write block ciphered)
ADDR ... address, 8 Bits (page or block address for page or block write)
CRC 1 ... cyclic redundancy check, 8 Bits (check sum of CMD and ADDR)
QUIT ... static confirmation, 3 Bits
DATA ... write data, 32 Bits (one page data)
CRC 2 ... cyclic redundancy check, 8 Bits (check sum of write data)

The write block command transmits one to four pages and the transponder confirms (QUIT) each of the blocks.

8.3. Transmission Transponder to Read/Write Device

8.3.1. Standard Protocol Mode

The parts of protocol transmitted by the transponder to the read/write device do not include any check sum because of flexibility reasons. To get the data integrity required by the application, check sums have to be calculated by the user software and stored together with the information in the transponder memory. This seems uncomfortable because the check sums use a little part of the available memory space in the transponder. The advantage of this solution is the flexibility to choose large checksums for applications requiring high data integrity and smaller check sums for applications requiring short access times which means short protocols.

8.3.2. Advanced Protocol Mode

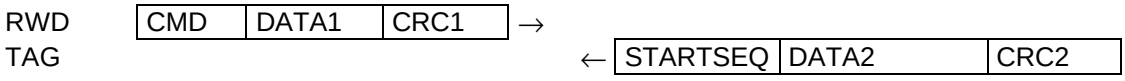
In Advanced Protocol Mode the parts of the select command, the read page command and the read block command, transmitted by the transponder to the read/write device, include a check sum.

The generator polynomial for this CRC reads:

$$u^8 + u^4 + u^3 + u^2 + 1 \quad = \quad 0x1D$$

and the CRC preassignment is 0xFF

The following explanation shows the feature of this protocol mode to provide a CRC in those commands.



TAG	...	transponder
RWD	...	read/write device
CMD	...	command, 4 Bits (read page, read block, read page ciphered, read block ciphered) or 5 Bits (select)
DATA1	...	32 Bits serial number for select, 8 Bits address for page or block read (ciphered or plain)
CRC1	...	cyclic redundancy check, 8 Bits (check sum of CMD and DATA1), calculated by the read/write device, checked by the transponder
STARTSEQ	...	start sequence of the transponder (6 ones)
DATA2	...	read data, 32 Bits to 128 Bits (one to four pages for page or block read)
CRC2	...	cyclic redundancy check, 8 Bits (check sum of DATA2, excluding STARTSEQ.), calculated by the transponder, checked by the read/write device.

8.4. Source Code for CRC-Checksum

The following lines of C-Code show an example for a CRC-Calculation.

```
/*************************************************************/
/*  _calc_CRC                                                */
/*  CRC-Calculation                                          */
/*                                                           */
/*  Input    BYTE idata *dptr, Startpointer points to the first */
/*                             byte of data                  */
/*           BYTE bitanz       Total number of data-bits     */
/*                             (byte alignment not necessary)*/
/*                                                           */
/*  Return   Byte crc          CRC-Value                     */
/*************************************************************/
#define  CRC_PRESET   0xFF
#define  CRC_POLYNOM  0x1D

BYTE  _calc_CRC (BYTE idata *dptr, BYTE bitanz)
{
     BYTE      crc, crc_in;
     BYTE      loop, tmp;


     crc_in = *dptr;
     crc = CRC_PRESET;
     for (loop=1; loop<=bitanz; loop++)
     {
          tmp = ((crc_in^crc)&0x80)? CRC_POLYNOM : 0x00;
          crc <<= 1;
          crc ^= tmp;
          crc_in <<= 1;
          if (!(loop&0x07)) crc_in = *(dptr+(loop>>3));
     }
     return (crc);
}
```

INTENTIONALLY LEFT BLANK

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, 04547-130
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: Al. Vicente Pinzon, 173 - 6th floor,
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

SCB52

PHILIPS