DATA SHEET

HT2 Transponder Family

Communication Protocol
Reader ⇔ HITAG™2 Transponder

Product Specification
Revision 2.1
Confidential

October 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 11
3.5. Switching the transmission direction 13
3.6. Data Integrity Using the HITAG 2 13

4. Command Set and Timing 14

4.1. Dataflow Read/Write Device ⇔ Transponder 14
4.2. START_AUTH-Instruction 14
4.2.1. Crypto Mode 15
4.2.2. Password Mode 16
4.2.3. Public Modes A and B 17
4.2.4. Public Mode C 19
4.3. Communication Instructions 20
4.3.1. Read Page 20
4.3.2. Read Page Inverted 21
4.3.3. Write Page 22
4.3.4. Halt 23

5. Memory Map 24

5.1. Crypto Mode.....24
5.2. Password Mode.....24
5.3. Definition of Passwords and Keys.....25
5.4. Operation Modes and Configuration.....26
5.4.1. Modes of Operation.....26
5.4.2. Status Flow.....27
5.4.3. Organizing the Configuration Byte.....28

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.
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 2 transponders are highly integrated and do not need any external components beside the HITAG 2 TAG ASIC (HT2 ICS20 02x) and one coil. The memory of the transponder has a size of 256 bits.

2. Introduction

The HITAG 2 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.

Using the configuration page custom specific configuration of the transponder is possible, modes and access possibilities are selected. The pages of the transponder memory can be protected against read or write acces by setting corresponding memory flags.

The HITAG 2 TAG ASIC provides - besides password and crypto mode - the following three standard read only modes, that can be configured using the configuration byte:

- public-mode-A (MIRO and transponders from µEM (H400x))
- public-mode-B (animal identification,according to ISO 11784 and ISO 11785)
- public-mode-C (PIT compatible mode PCF793x)

3. Specifications

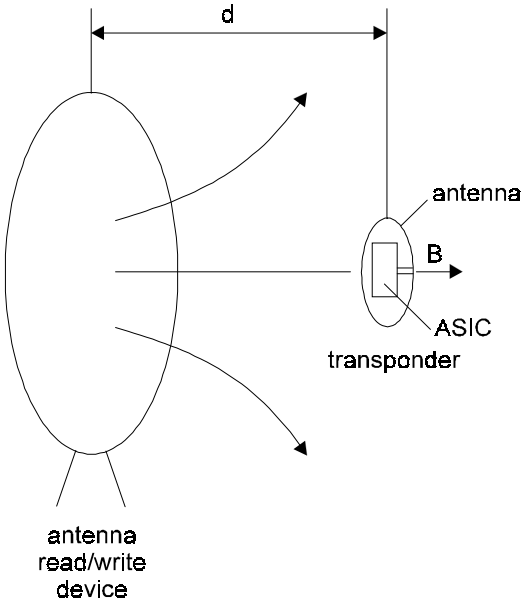
3.1. Transponders / Overview

parameter	
carrier frequency	125 kHz
coding read write	Manchester / Biphase Pulse Duration
modulation	ASK (amplitude shift keying)
total memory size	256Bit
user memory read/write	128 Bit
read only serial number	32 bits
data retention	10 years
data security	encryption, authentication, passwords
data integrity	half-duplex handshake, reverse data transmission

3.2. Electromagnetic Characteristics

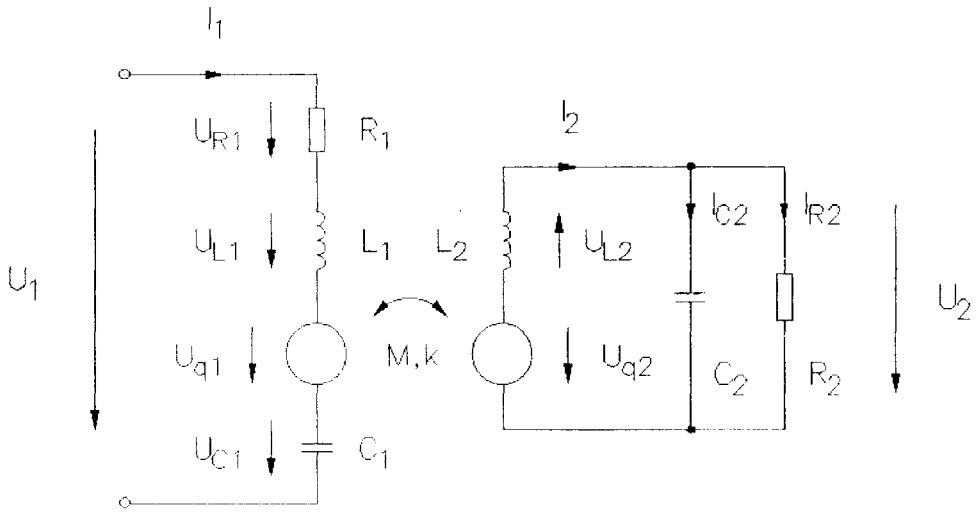
3.2.1. Magnetic Flux Densities

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

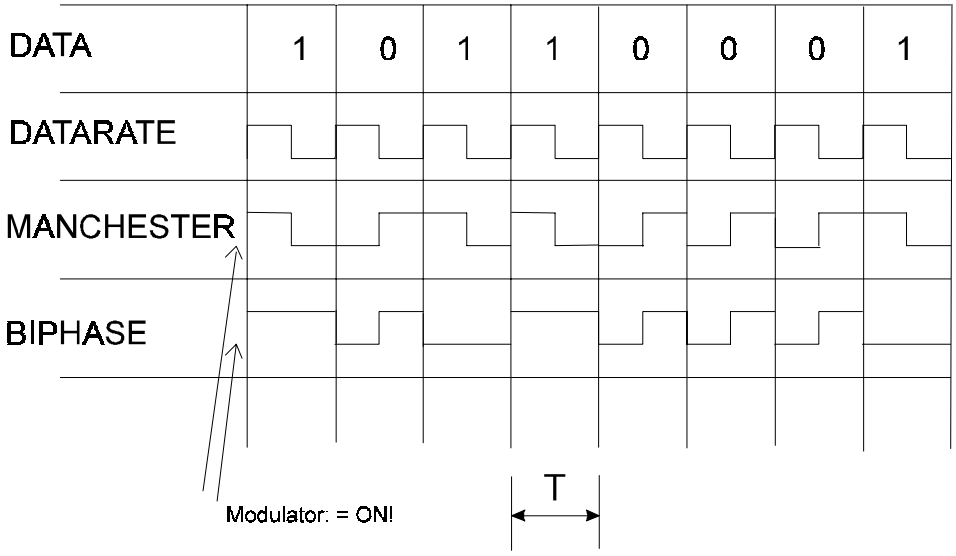
3.3.1. Coding

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 different codes are used for the transmission of data to the read/write device:

Mode	Coding	Bit Length T	Bit rate
Crypto	Biphase/Manchester	32 T_0	4 KBit/s
Password	Biphase/Manchester	32 T_0	4 KBit/s
Public Mode A (µEM H400x)	Manchester	64 T_0	2 KBit/s
Public Mode B	Biphase	32 T_0	4 KBit/s
PCF793X (PIT)	Biphase	64 T_0	2 KBit/s

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

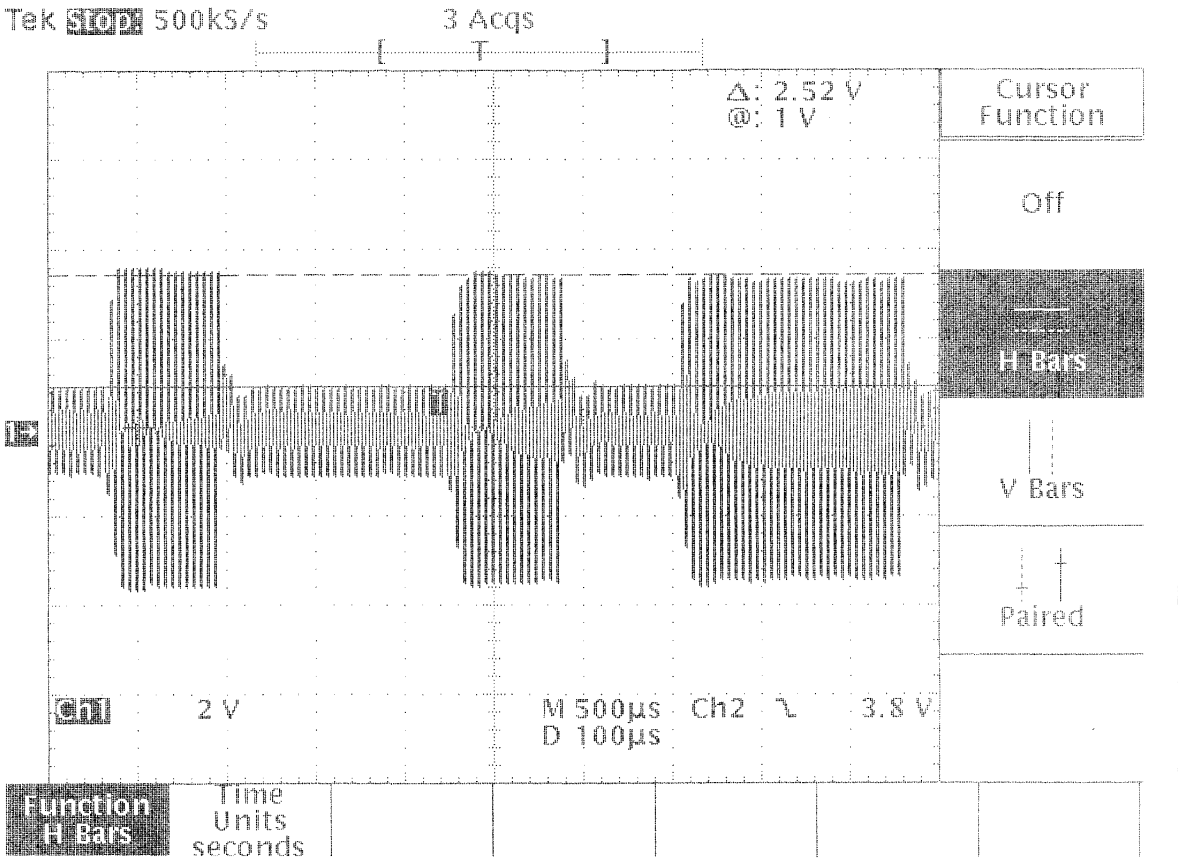


The first bit of the transmitted data always starts with the Modulator ON (loaded) state.

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

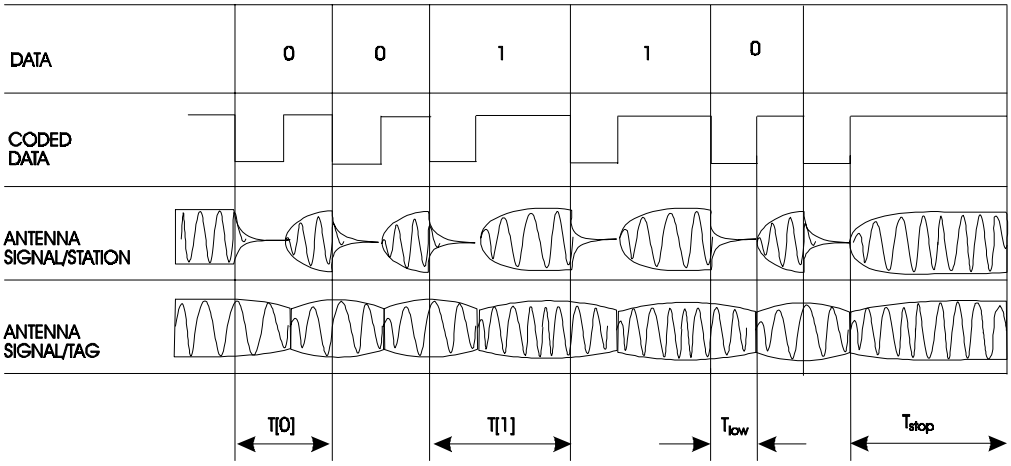
Data are transmitted to the transponder by switching on/off the current through the antenna. When the current is switched off, the physical state is named low field, otherwise high field.

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:

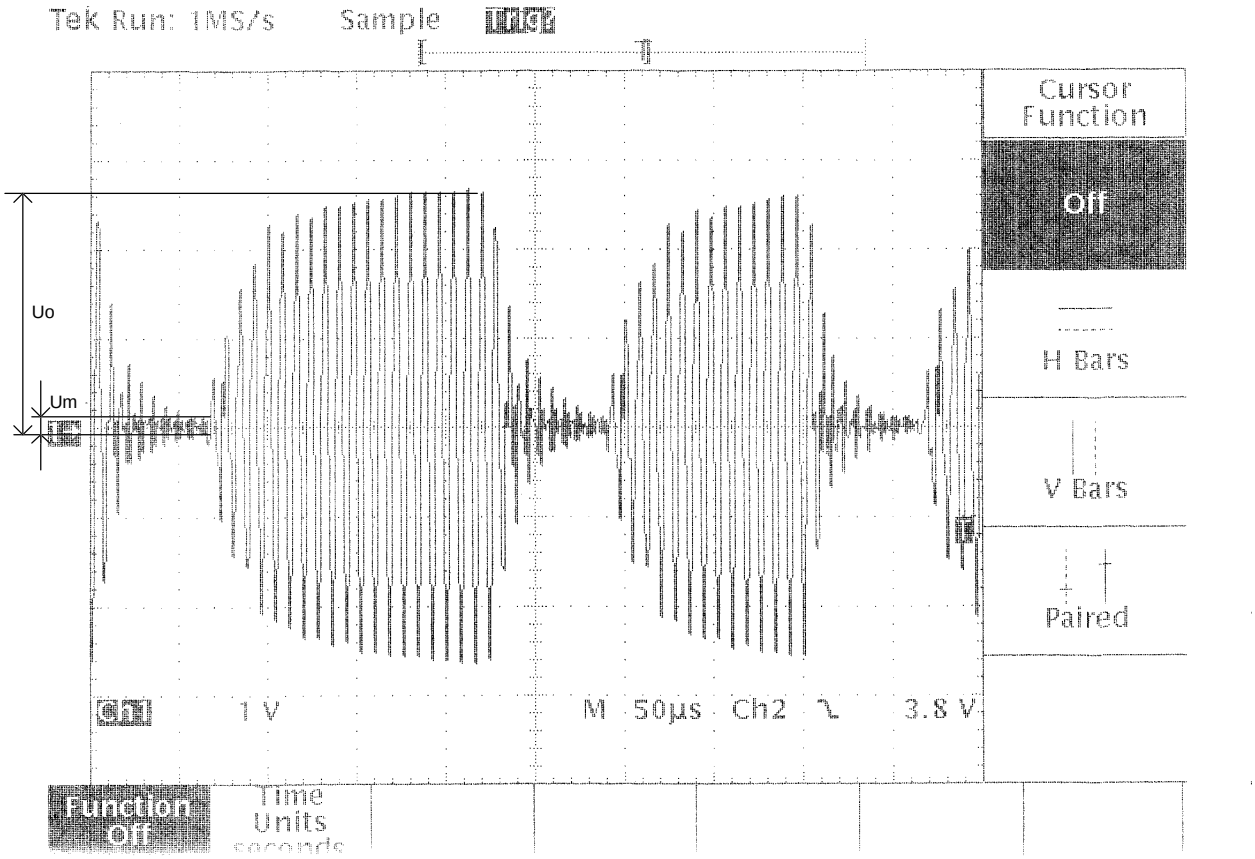
Symbol	Description	Duration
t_{low}	low field time	8 T_0
T[0]	logic 0 pulse length	22 T_0
T[1]	logic 1 pulse length	28 T_0

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).
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. 199 T_0...max 206 T_0
t_{WAIT2}	transponder switching from transmit to receive, wait time after end of data	min. 90 T_0 *)

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

3.6. Data Integrity Using the HITAG 2

For data transmission between read/write device and transponders the HITAG 2 supports special commands to increase data integrity.
Using additional inverted data transmission for commands, addresses as well as read data, utmost data integrity is achieved.
For write transmissions read after write is recommended.
See also Chapter 4, Command Set and Timing.

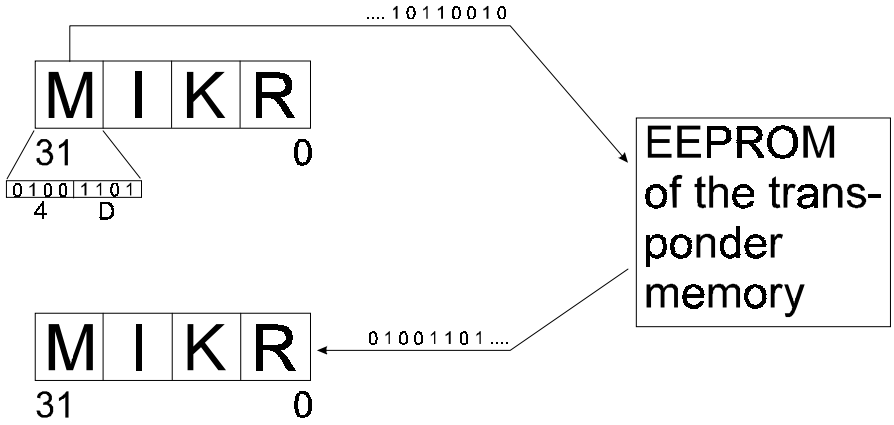
4. Command Set and Timing

There are two types of instructions

1. Instruction for the beginning of the communication (START_AUTH)
2. Instructions for the communication

4.1. Dataflow Read/Write Device ⇔ Transponder

Please note that the transponder memory works like a FIFO (First-In-First-Out) memory. Therefore the order of the bits transferred is as described in the example below:



Write: Bit 31 is sent first to the transponder.
Read: Bit 31 is sent first to the read/write device.

4.2. START_AUTH-Instruction

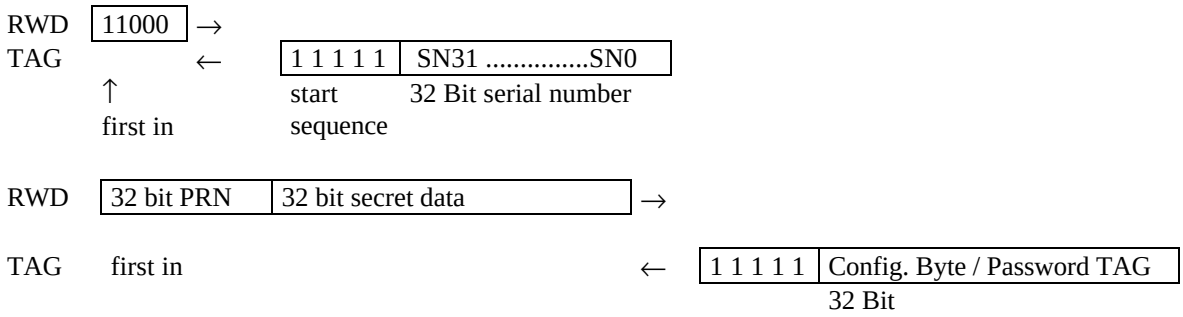
CM1	CM0	ADDR4	ADDR3	ADDR2
1	1	0	0	0

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).

4.2.1. Crypto Mode

After an instruction START_AUTH from the read/write device (RWD) all transponders (TAGs) in the field respond with a start sequence (5 bits „1“) followed by their 32 bit ID number.



The instruction START_AUTH cannot be repeated, because at the same time the crypto unit is initialized. A second START_AUTH resets the statemachine. Therefore the transponder only responds to every second START_AUTH.

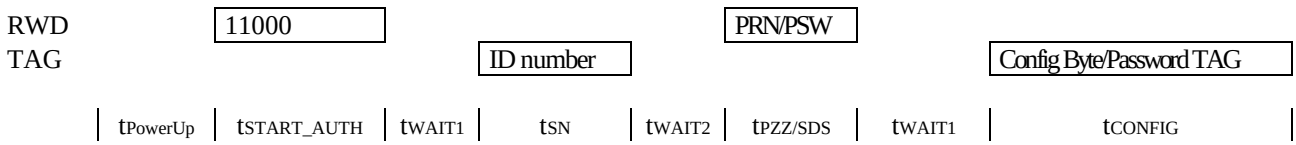
After the transponder has sent the serial number, the read/write device sends a 32 bit Pseudo Random Number (PRN) and a 32 bit secret datastream to the transponder. If the secret datastream corresponds with the secret datastream on the transponder, Page 3 of the transponder (8 bit configuration, 24 bit password transponder) is transmitted after the 5 bit header.

With the transponder password in the configuration page the mutual authentication takes place.
Access to the transponder is only possible after this mutual authentication and password checking routine. Transmission of the password and the following communication takes place enciphered.

As the information about the configuration of the transponder (password or crypto) is transmitted with the configuration page, the read/write device must know which type of transponder has to be handled. In one application either crypto transponders or password transponders are to be handled.

The write instructions are interrupted by the transponder (TAG), when the EEPROM supply is too low during write.

Timing:

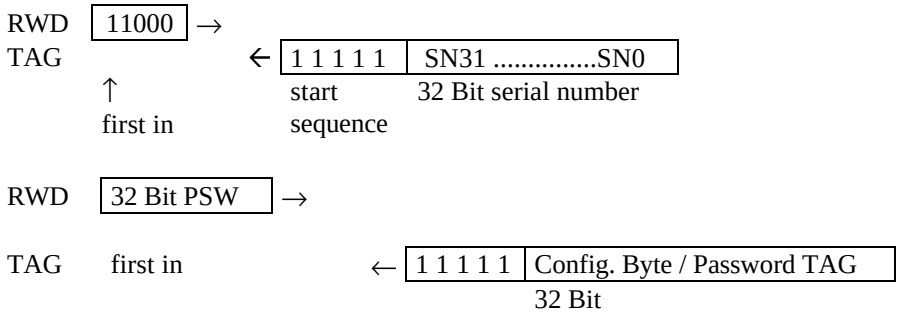


	MIN	TYP	MAX	Unit
$t_{PowerUp}$		312.5		T_0
t_{START_AUTH}		116		T_0
t_{WAIT1}	199		206	T_0
t_{SN}		1184		T_0
t_{WAIT2}	90			T_0
$t_{PZZ/SDS}$	1280	1536	1792	T_0
t_{CONFIG}		1184		T_0
total		4630		T_0

After a following t_{WAIT2} the first read or write instruction can be sent by the read/write device. The authentication time in crypto mode is about 4630 T_0.

4.2.2. Password Mode

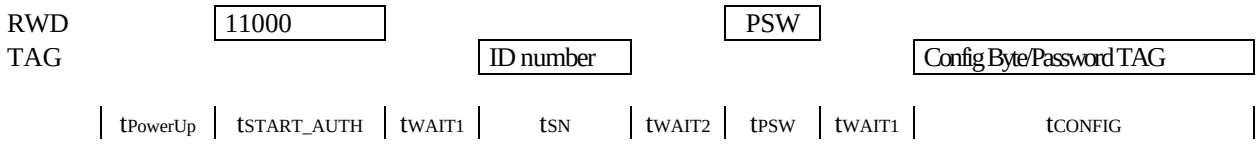
After an instruction START_AUTH from the read/write device (RWD) all transponders (TAGs) in the field respond with a start sequence (5 bits "1") followed by their 32 bit serial number.



The instruction START_AUTH cannot be repeated. A second START_AUTH resets the statemachine. Therefore the transponder only responds to every second START_AUTH.
After the transponder has sent the serial number, the read/write device sends a 32 bit password (PSW). If the password corresponds with the password on the transponder, Page 3 of the transponder (8 bit configuration, 24 bit password transponder) is transmitted after the 5 bit header.

With the transponder password in the configuration page the mutual authentication takes place.
Access to the transponder is only possible after this mutual authentication and password checking routine.
As the information about the configuration of the transponder (password or crypto) is transmitted with the configuration page, the read/write device must know which type of transponder has to be handled. In one application either crypto transponders or password transponders are to be handled.
The read and write instructions are interrupted by the transponder, when the EEPROM supply is too low during read or write.
As the transponder is selected by the password, each transponder must have a unique password, that can have a connection with the serial number.

Timing:



	MIN	TYP	MAX	Unit
$t_{PowerUp}$		312.5		T_0
t_{START_AUTH}		116		T_0
t_{WAIT1}	199		206	T_0
t_{SN}		1184		T_0
t_{WAIT2}	90			T_0
t_{PSW}	640	768	896	T_0
t_{CONFIG}		1184		T_0
total		3860		T_0

After t_{WAIT2} the first read or write instruction can be sent by the read/write device. The authentication time in password mode is about 3860 T_0.

4.2.3. Public Modes A and B

After the configuration byte is stored in the logic during power up, and after the synchronisation phase of the statemachine, the transponder waits for the instruction START_AUTH. If the read/write device does not send the instruction START_AUTH within $t_{WAIT\ START\_AUTH}$ after the Power_Up (312.5 T_0 after the RF-field is applied) the transponder begins to send the data in one of the public modes (depending on the configuration).

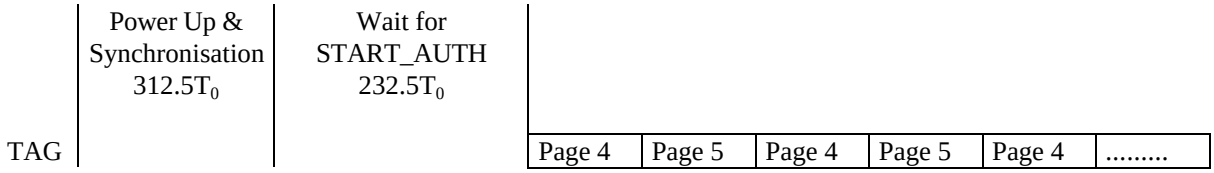
Symbol	Description	Duration
$t_{PowerUp}$	internal power_up time	312.5 T_0
$t_{WAIT\ START\_AUTH}$	waiting time to receive the START_AUTH command	**max.** 232.5 T_0*)

*) If the waiting time $t_{WAIT\ START\_AUTH}$ exceeds 232.5 T_0 the transponder enters the *read-only* state.

Public Mode A

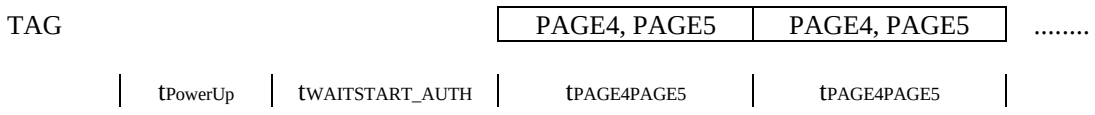
In this standard read-only mode the transponder (TAG) cyclically transmits page 4 and page 5 in plain mode to the read/write device without a start sequence as long as the TAG is in the field of the read/write device. The data are transmitted in Manchester Code with a baudrate of 2 KBit/s.

With the help of this mode µEM transponders of the H400x family are emulated.



Note : As the read/write device has to be synchronized to the data, the first 9 bits of page 4 are "1" (header of the transponder in Public Mode A).

Timing:



	MIN	TYP	MAX	Unit
$t_{PowerUp}$		312.5		T_0
$t_{WAIT\ START\_AUTH}$			232.5	T_0
$t_{PAGE4PAGE5}$		4096		T_0
total		4640		T_0

If the read/write device sends the instruction START_AUTH within the 232.5 T_0 after the power up the transponder behaves like a normal HITAG 2. Depending on bit 3 of the configuration byte, the communication is plain or encrypted.

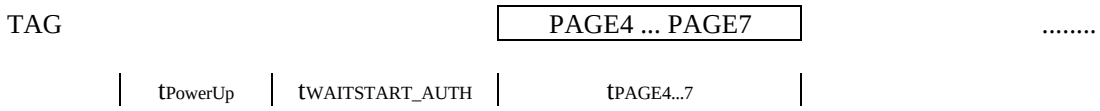
Public Mode B:

Public Mode B accords to the ISO standards 11784 and 11785 for animal identification.
In this mode the transponder cyclically transmits page 4 to page 7 in plain mode to the read/write device without a start sequence as long as the transponder is in the field of the read/write device. The data are transmitted in Biphase Code with a baudrate of 4 KBit/s.

	Power Up & Synchronisation $312.5T_0$	Wait for START_AUTH $232.5T_0$					
TAG			Page 4	Page 5	Page 6	Page 7	Page 4	.....

If the read/write device sends the instruction START_AUTH within the 232.5 T_0 after the power up the transponder behaves like a normal HITAG 2. Depending on bit 3 of the configuration byte, the communication is plain or encrypted.

Timing:



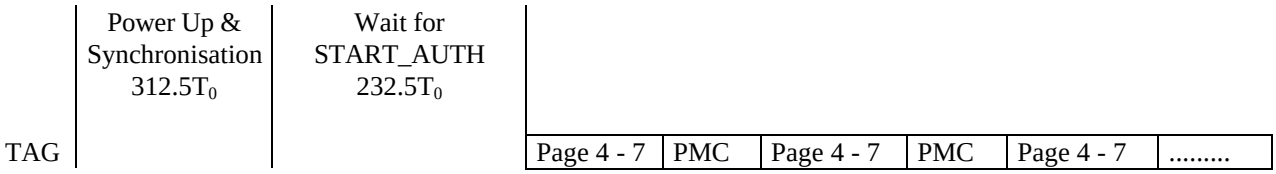
	MIN	TYP	MAX	Unit
tPowerUp		312.5		T_0
tWAITSTART_AUTH			232.5	T_0
tPAGE4...7		4096		T_0
total		4640		T_0

4.2.4. Public Mode C

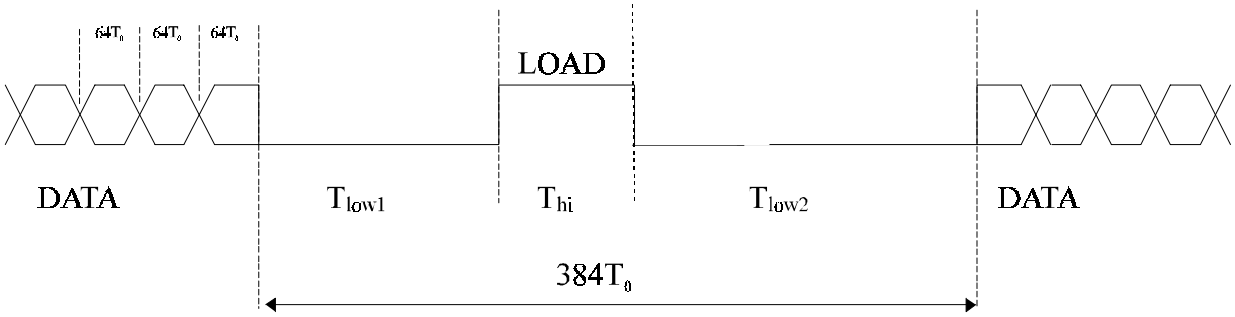
With this additional feature a HITAG 2 that is configured in Public Mode C is compatible to the PCF793X (PIT).

After the configuration byte is stored in the logic during power up, and after the synchronisation phase of the statemachine, the transponder (TAG) waits for the instruction START_AUTH. If the read/write device does not send the instruction START_AUTH within 232.5 T_0 after power up the transponder begins to send the data in PCF793X mode.

In this mode the transponder cyclically transmits page 4 to page 7 in plain mode to the read/write device without a start sequence as long as the transponder is in the field of the read/write device. The data are transmitted in Biphase Code with a baudrate of 2 KBit/s. Between the 128 bit datablocks there is a Program Mode Check phase (PMC).



Program Mode Check Phase:

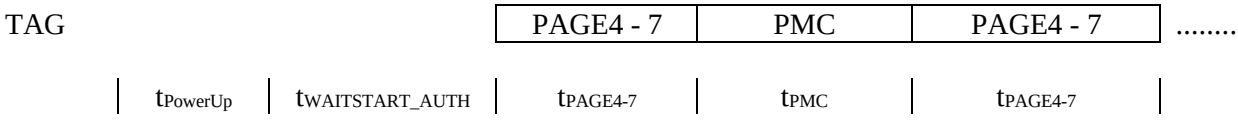


T_{hi} = 64 T_0
T_{low1} = 128 T_0
T_{low2} = 192 T_0

If the read/write device sends the instruction START_AUTH within the 232.5 T_0 after the power up the transponder behaves like a normal HITAG 2. Depending on bit 3 of the configuration byte, the communication is plain or encrypted.

Note : Only the READ MODE of the PCF793X is emulated (with a different PMC).

Timing:



	MIN	TYP	MAX	Unit
$t_{PowerUp}$		312.5		T_0
$t_{WAITSTART\_AUTH}$			232.5	T_0
$t_{PAGE4-7}$		8192		T_0
t_{PMC}		384		T_0
total		9120		T_0

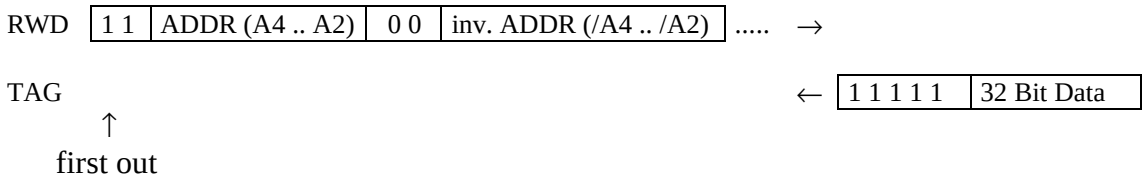
4.3. Communication Instructions

Before starting a read or write operation the transponder has to be selected by the START_AUTH command.

CM1	CM0	ADDR4	ADDR3	ADDR2	command
1	1	x	x	x	READ PAGE
0	1	x	x	x	READ PAGE INVERTED
1	0	x	x	x	WRITE PAGE
0	0	x	x	x	HALT

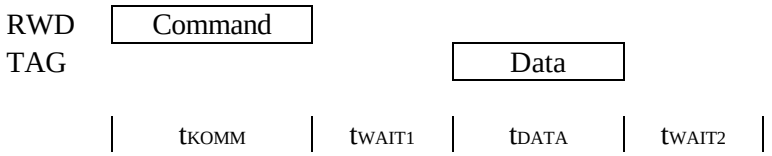
Times for communication instructions depend on the protection of data in the protocol from read/write device to transponder.

4.3.1. Read Page



The instruction READ PAGE (2 bits) and the page address (3 bits) are transmitted to the transponder in normal mode and in inverted mode to secure the data channel from read/write device to transponder. To achieve a higher security level, this protocol can be repeated several times. The logic on the transponder checks if there is a failure in the sequence. The READ PAGE instruction therefore is 10, 15, 20, ... bits long. If there is a failure in the transmission of the sequence the transponder is reset and the communication has to be started again with START_AUTH. If the transponder receives no more data and there was no failure in the transmission of the sequence, the transponder answers with the 5 bit header and the 32 bit data of the addressed page.

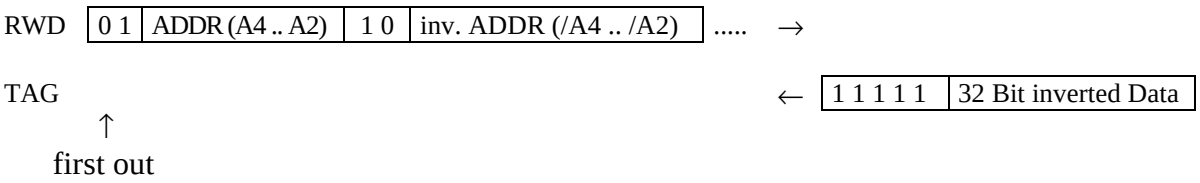
Timing:



	MIN	TYP	MAX	Unit
t_{KOMM}		240		T_0
t_{WAIT1}	199		206	T_0
t_{DATA}		1184		T_0
t_{WAIT2}	90			T_0
total		1750		T_0

After t_{WAIT2} the next instruction can be accepted by the transponder.
A typical READ PAGE (10 bit command) time therefore is: 1750 T_0

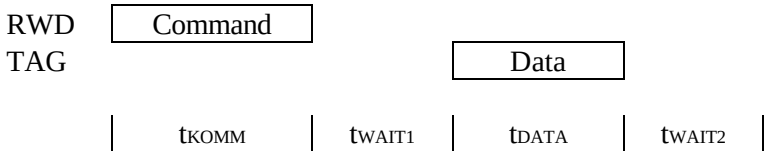
4.3.2. Read Page Inverted



The instruction READ PAGE INVERTED (2 bits) and the page address (3 bits) are transmitted to the transponder in normal mode and in inverted mode to secure the data channel from read/write device to transponder. To achieve a higher security level, this protocol can be repeated several times. The logic on the transponder checks if there is a failure in the sequence. The READ PAGE INVERTED instruction therefore is 10, 15, 20, ... bits long. If there is a failure in the transmission of the sequence the transponder is reset and the communication has to be started again with START_AUTH. If the transponder receives no more data and there was no failure in the transmission of the sequence, the transponder answers with the 5 bit header and the 32 bit data of the addressed page. The data are transmitted inverted to the read/write device.

By alternating transmission of the instructions READ PAGE and READ PAGE INVERTED the data from the transponder to the read/write device can be secured at a level that can be choosen by the user. Additionally check data can be stored in the EEPROM with the data.

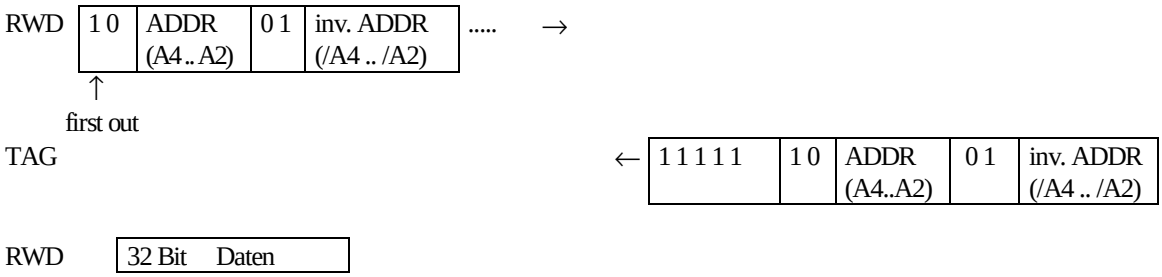
Timing:



	MIN	TYP	MAX	Unit
t_{KOMM}		240		T_0
t_{WAIT1}	199		206	T_0
t_{DATA}		1184		T_0
t_{WAIT2}	90			T_0
total		1750		T_0

After t_{WAIT2} the next instruction can be accepted by the transponder.
A typical READ PAGE INVERTED (10 bit command) time therefore is: 1750 T_0

4.3.3. Write Page

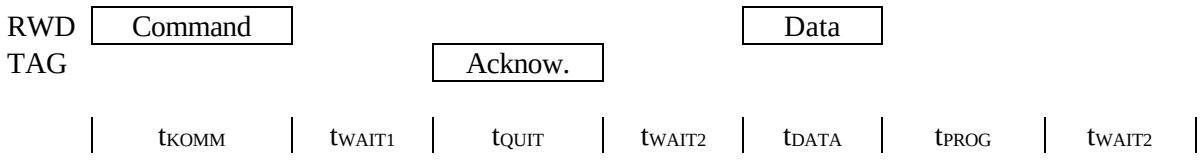


The instruction WRITE (2 bits) and the page address (3 bits) are transmitted to the transponder in normal mode and in inverted mode to secure the data channel from read/write device to transponder. To achieve a higher security level, this protocol can be repeated several times. The logic on the transponder checks if there is a failure in the sequence. The WRITE instruction therefore is 10, 15, 20, ... bits long. If there is a failure in the transmission of the sequence the transponder is reset and the communication has to be started again with START_AUTH. If the transponder receives no more data and there was no failure in the transmission of the sequence, the transponder answers with the 5 bit header and an acknowledgement. This acknowledgement consists of the WRITE instruction and the page address in normal and inverted mode.
With this procedure the read/write device knows, that the data are written to the correct address.

After the address sent from transponder to read/write device has been checked, the read/write device transmits 32 bit data to the transponder. There is no acknowledgement from the transponder concerning the success of data programming. This can only be tested by read-after-write.

The READ command for a read-after-write has to be executed immediately following the WRITE command. If the EEPROM supply was too low during programming (insufficiently programmed cell, data retention not ensured) the read command is not executed by the transponder (control function!). In this case the transponder is reset and the user has to start again with a START_AUTH command.

Timing:



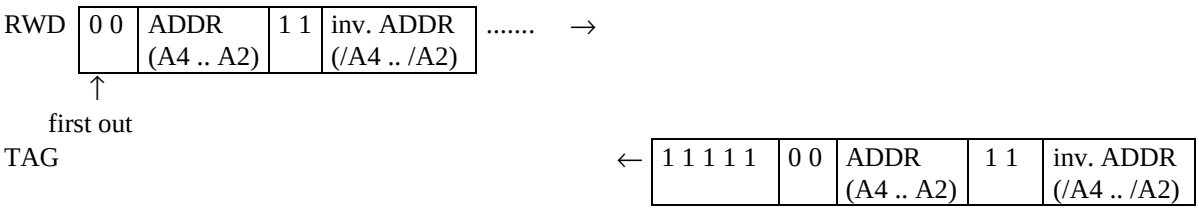
	MIN	TYP	MAX	Unit
t_{KOMM}		240		T_0
t_{WAIT1}	199		206	T_0
t_{QUIT}		480		T_0
t_{WAIT2}	90			T_0
t_{DATA}	640	768	896	T_0
t_{PROG}		614		T_0
t_{WAIT2}	90			T_0
total		2500		T_0

After t_{WAIT2} the next instruction can be accepted by the transponder.
A typical WRITE PAGE (10 bit command) time therefore is: 2500 T_0

4.3.4. Halt

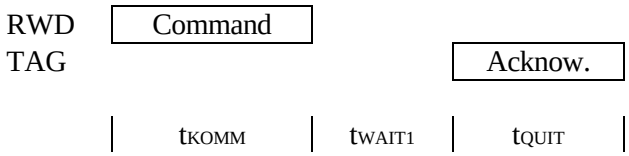
With the HALT instruction a selected transponder can be set to the HALT mode. In this mode the transponder is muted and does not respond to a START_AUTH from the read/write device. If the transponder is set to HALT mode after the communication, other transponders within the field of the antenna can be handled.

If the transponder is in HALT mode, only a Power-on-reset (POR) enables the transponder to communicate with the read/write device again. This means that the transponder has to leave the field of the antenna or the field has to be switched off (Reset).



The instruction HALT (2 bits) and the page address (3 bits) are transmitted to the transponder in normal mode and in inverted mode to secure the data channel from read/write device to transponder. To achieve a higher security level, this protocol can be repeated several times. The logic on the transponder checks if there is a failure in the sequence. The HALT instruction therefore is 10, 15, 20, ... bits long. If there is a failure in the transmission of the sequence the transponder is reset and the communication has to be started again with START_AUTH. If the transponder receives no more data and there was no failure in the transmission of the sequence, the transponder answers with the 5 bit header and an acknowledgement. This acknowledgement consists of the HALT instruction and the page address in normal and inverted mode. The address that is transmitted with the HALT instruction can be any of the possible addresses.

Timing:



	MIN	TYP	MAX	Unit
t_{KOMM}		240		T_0
t_{WAIT1}	199		1648	T_0
t_{QUIT}		480		T_0
total		1000		T_0

A typical HALT (10 bit command) therefore is 1000 T_0.

5. Memory Map

The memory of the transponder consists of 256 bits EEPROM memory and is organized in 8 pages with 32 bits each.

Depending on the operation mode the EEPROM is organized as described in the following.

5.1. Crypto Mode

Page	Content
0	Serial Number
1	32 bit "KEY LOW"
2	16 bit " KEY HIGH", 16 bit reserved
3	8 bit Configuration, 24 Bit Password TAG
4	read/write page
5	read/write page
6	read/write page
7	read/write page

5.2. Password Mode

Page	Content
0	Serial Number
1	Password RWD
2	reserved
3	8 bit Configuration, 24 bit Password TAG
4	read/write page
5	read/write page
6	read/write page
7	read/write page

5.3. Definition of Passwords and Keys

Keys are cryptographic codes, which determine data encryption during data transfer between read/write device and transponder. They are used to select a HITAG 2 transponder in Crypto Mode. The 16 bit KEY HIGH and 32 bit KEY LOW form one 48 bit key which has to be identical on both the transponder and the read/write device.

Passwords are needed to select a HITAG 2 transponder in Password Mode. There is one pair of passwords (Password TAG, Password RWD) which has to be identical both on the transponder and the read/write device.

Password TAG: Password that the transponder sends to the read/write device and which may be verified by the latter (depending on the configuration of the read/write device).

Password RWD: Password that the read/write device sends to the transponder and which is checked for identity by the latter.

It is important that the following values are in accordance with each other, i.e. the respective data on the read/write device and on the transponder have to be identical pairs.

HITAG 2 in Password mode:

on the read/write device		**on the transponder**
Password RWD	⇔	Password RWD

as an option (depending on the configuration of the read/write device):

Password TAG	⇔	Password TAG

HITAG 2 in Crypto mode:

on the read/write device		**on the transponder**
KEY LOW	⇔	KEY LOW
KEY HIGH	⇔	KEY HIGH

as an option (depending on the configuration of the read/write device):

Password TAG	⇔	Password TAG

The passwords and keys are predefined by Philips Semiconductors by means of defined Transport Passwords and a Transport Key. They can be written to, which means that they can be changed (see also Chapter “Configuration of Delivered HITAG 2 Transponders“).

ATTENTION: Passwords and Keys only can be changed if their current values are known!

5.4. Operation Modes and Configuration

With the Configuration Byte the operation mode and the access rights to the memory can be selected. During Power-Up of the transponder the Configuration Byte is read from the transponder's EEPROM.

If you change the configuration, keys or passwords, you have to place the transponder directly on the antenna or hold it directly to it (0-distance)! In order to avoid any errors do not move the transponder during this write process and be sure that you are in a safe environment without electrical noise.

5.4.1. Modes of Operation

The HITAG 2 can be operated in several modes.

Crypto Mode:

Mode for writing or reading the transponder with encrypted data transmission.

Password Mode:

Mode for writing or reading the transponder with plain data transmission after password check.

Public Mode A (Manchester):

Read only mode emulating Philips Semiconductors´ MIRO transponders resp. µEM H400x transponders.
The 64 bits of the user Pages 4 and 5 are cyclically transmitted to the read/write device.

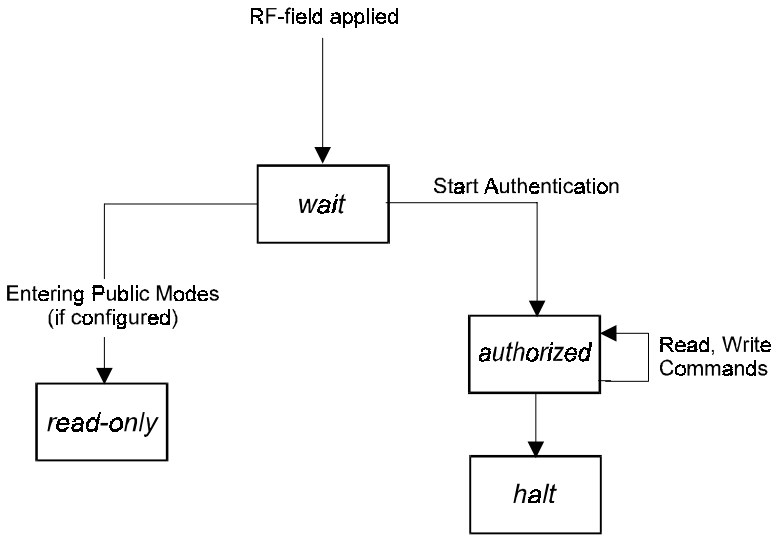
Public Mode B (Biphase):

Read only mode according to ISO standards 11784 and 11785 for animal identification.
The 128 bits of the user Pages 4 to 7 are cyclically transmitted to the read/write device.

Public Mode C (Biphase):

Read only mode emulating the read operation of the PCF793X (with a slightly different Program Mode Check).
In the Public Mode C the 128 bits of the user Pages 4 to 7 are cyclically transmitted to the read/write device.

5.4.2. Status Flow



After entering the RF-field the transponder waits for a command to start the authentication.

After issuing this command the mutual authentication takes place, followed by read- and write commands.
In password mode the data transfer occurs plain, in crypto mode data are encrypted.

The halt mode can be entered for muting a transponder.

If the transponder is configured in one of the public modes, these modes are entered automatically after a certain waiting time and data pages are sent cyclically to the read/write device.

By issuing the command to start the authentication during the waiting time also public mode transponders can be brought into the authorized state.

5.4.3. Organizing the Configuration Byte

The Configuration Byte is represented by the first 8 bits of Page 3 of the transponder memory.

5.4.3.1. Configuration Byte:

7	6	5	4	3	2	1	0

0: Manchester Code
1: Biphase Code

Bit 2	Bit 1	Version	Coding	Coding in HITAG 2-Operation
0	0	Public Mode B	biphase	depending on bit 0
0	1	Public Mode A	manchester	depending on bit 0
1	0	Public Mode C	biphase	depending on bit 0
1	1	HITAG 2	depending on bit 0	depending on bit 0

0: password mode
1: crypto mode

0: PAGE 6 and 7 read/write
1: PAGE 6 and 7 read only

0: PAGE 4 and 5 read/write
1: PAGE 4 and 5 read only

THE SETTING OF THIS BIT IS **OTP !**
0: PAGE 3 read/write
1: PAGE 3 read only; Configuration Byte and Password TAG **fixed**

THE SETTING OF THIS BIT IS **OTP !**
0: PAGE 1 and 2 read/write
1: PAGE 1 no read/no write
PAGE 2 read only (when transponder is in password mode)
PAGE 2 no read/no write (when transponder is in crypto mode)

Configuration Byte / Bit 6:

Bit 6 = ‘0’: Page 3 is read/write.
Bit 6 = ‘1’: Page 3 can only be read. This process is irreversible !

ATTENTION: Do not set Bit 6 of the Configuration Byte to ‘1’ before having written the final data into Page 3 (including the Configuration Byte and Password TAG) of the transponder.

Configuration Byte / Bit 7:

Bit 7 = ‘0’: Pages 1 and 2 are read/write.
Bit 7 = ‘1’: Pages 1 and 2 are locked against writing. This process is irreversible !

ATTENTION: Do not set Bit 7 of the Configuration Byte to ‘1’ before having written the final data into Pages 1 and 2 of the transponder.

5.4.3.2. Standard values for the Configuration Byte:

Password Mode	:	0x06
Crypto Mode	:	0x0E
Public Mode A	:	0x02
Public Mode B	:	0x00
Public Mode C	:	0x04

5.4.3.3. Configuration of Delivered HITAG 2 Transponders

HITAG 2 transponders are delivered with the following configuration by Philips Semiconductors:

Unique Serial Number:

Serial Number:	Read Only	-	fixed

Configuration Byte:

0x06:	Password Mode (Manchester Code)	-	can be changed
	Page 6 and 7 read/write	-	can be changed
	Page 4 and 5 read/write	-	can be changed
	Page 3 read/write	-	can be changed
	Page 1 and 2 read/write	-	can be changed

Values for Transport Passwords, Transport Keys:

Password RWD:	0x4D494B52	(= ″MIKR″)
Password TAG:	0xAA4854	
Key Low:	0x4D494B52	(= ″MIKR″)
Key High:	0x4F4E	(= ″ON″)

RECOMMENDATION:

Before delivering transponders to end users, Pages 1 to 3 should be locked (set Configuration Byte / Bit 6 to ‘1’ for Page 3 and set Configuration Byte / Bit 7 to ‘1’ for Pages 1 and 2).

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