HITAG 2

Transponder IC

Rev. 3.0 — 26 February 2010
188330

Product data sheet
CONFIDENTIAL

1. Introduction

HITAG 2 is part of the universal and powerful product line of NXP Semiconductors 125 kHz HITAG family. The contactless read/write system that works with passive transponders is suitable for various applications. Inductive coupling allows to achieve big reading ranges.

The HITAG product family is used in the proximity area (operating range up to about 200 mm) as well as in the long range area (operating range up to about 1000 mm).

2. General description

HITAG 2 based transponders are highly integrated and do not need any additional components beside the HITAG 2 transponder IC and the external coil.
Data are transmitted bidirectionally, in half duplex mode, between read/write device (RWD) and HITAG transponder IC.
To achieve a main stream security, data may be transmitted enciphered.

HTAG 2 transponder IC offer a memory of 256 bit.

Custom specific configuration of the transponder IC is possible by using the configuration page. The configuration page allows the selection of different modes and access possibilities and also the configuration of the memory. The pages of the memory can be protected against read or write access by setting corresponding memory flags.

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

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

3. Features and benefits

- Identification transponder for use in contactless applications
- Operating frequency 125 kHz
- Data transmission and energy supply via RF link, no internal battery
- Reading distance same as writing distance
- Non-volatile memory of 256 bits (128-bit user data and 128-bit control data/secret memory) organized in 8 pages, 4 bytes each
- 10 years non-volatile data retention
- 100 000 erase/write cycles
- Selective read/write protection of memory content
- Two coding schemes for read operation: Biphase and Manchester coding
- Effective communication protocol with outstanding data integrity check
- Mutual authentication function
- Read/write mode allows:
    - Plain data transmission (password mode)
    - Encrypted data transmission (crypto mode)
- In read/write mode multi-tag operation possible because of special HALT-function
- Emulation of standard industrial read-only transponders:
    - Public Mode A (MIRO and transponders from μEM (H400x))
    - Public Mode B (according to ISO 11784 and ISO 11785 for animal identification)
    - Public Mode C (PIT compatible mode)

4. Applications

- Logistics
- Livestock tracking
- Asset tracking
- Gas cylinder ID
- Casino - gambling
- Industrial automation

5. Ordering information

Table 1. Ordering information

Type number	Package			
	Name	Description	Type	Version
HT2ICS2002W/V9F	Wafer	sawn wafer on FFC, 150 µm, 8 inch, UV, inked and mapped	-	-
HT2MOA2S20/E/3	MOA2	plastic leadless module carrier package; 35 mm wide tape	-	SOT500-2
HT2DC20S20/F	PLLMC	plastic leadless module carrier package	-	SOT385-1

6. Block diagram

The HITAG 2 transponder IC requires no external power supply. The contactless interface generates the power supply and the system clock via the resonant circuitry by inductive coupling to the RWD. The interface also demodulates data transmitted from the RWD to the HITAG 2 transponder IC, and modulates the magnetic field for data transmission from the HITAG 2 transponder IC to the RWD.

Data are stored in a non-volatile memory (EEPROM). The memory has a capacity of 256 bit and is organized in pages.

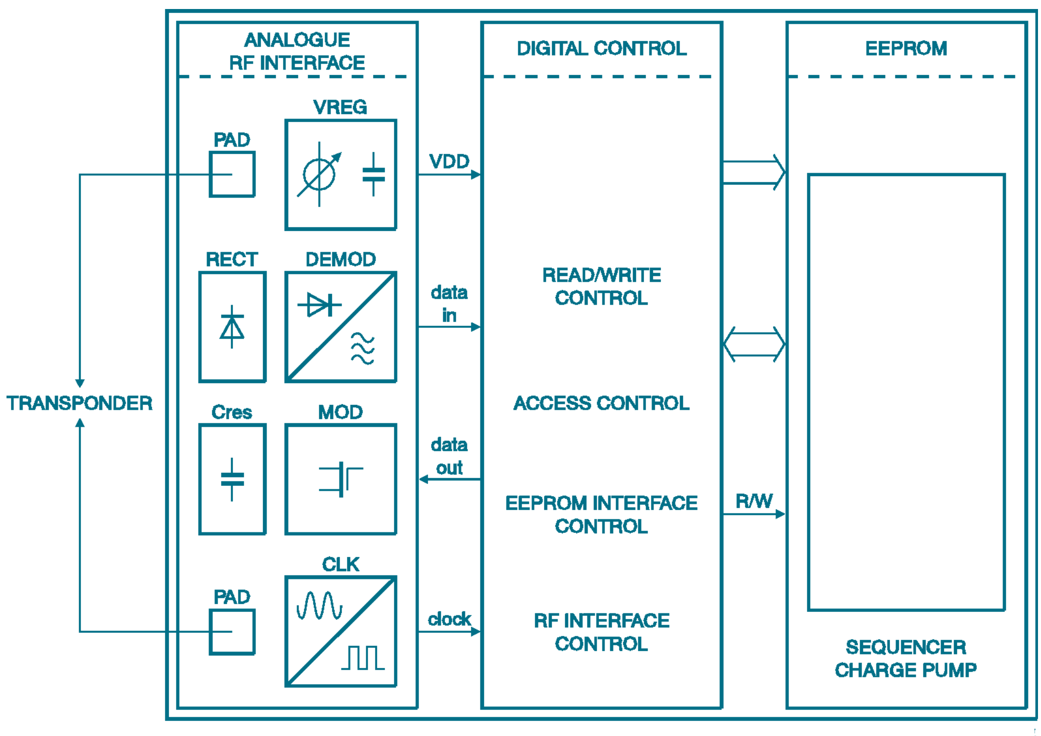


Fig 1. Block diagram of HITAG 2 transponder IC

7. Pinning information

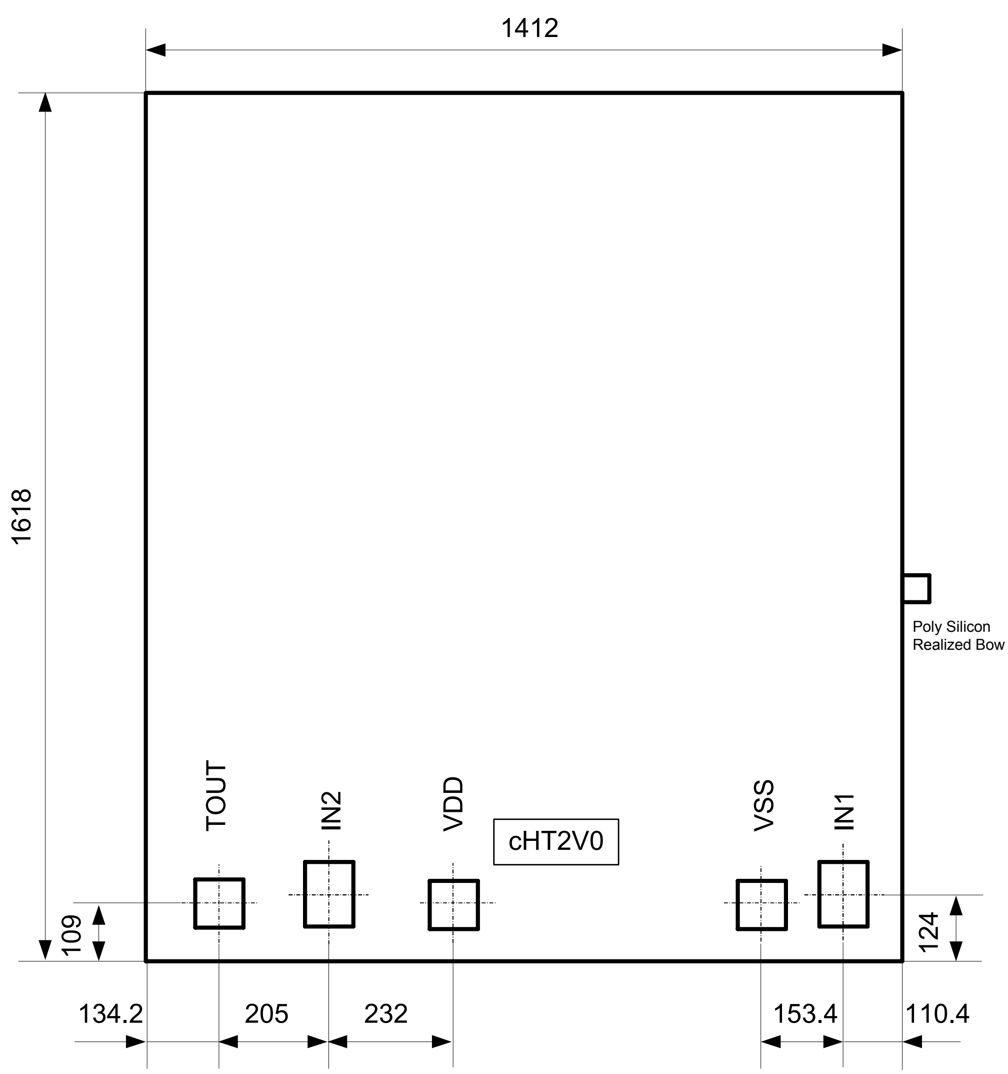


Fig 2. Bond plan of HT2ICS2002 [units in μm]

8. Mechanical specification

8.1 Wafer specification

See Ref. 2 "General specification for 8'' wafer on UV-tape".

8.1.1 Wafer

- Designation: each wafer is scribed with batch number and wafer number
- Diameter: 200 mm (8'')
- Thickness: 150 μm ± 15 μm
- Process: C150EE
- Batch size: 25 wafers
- PGDW: 11091

8.1.2 Wafer backside

- Material: Si
- Treatment: ground and etched
- Roughness: R_a max. 0.5 μm, R_t max. 5 μm

8.1.3 Chip dimensions

- Die size without scribe: 1618 μm x 1412 μm = 2284616 μm
- Scribe line width:
  X-dimension: 108 μm
  Y-dimension: 102 μm
- Number of pads: 5

8.1.4 Passivation on front

- Type: single layer
- Material/Thickness: TEOS 300 nm, Nitride 700nm

8.1.5 Bondpads

- Pad size:
  – IN1, IN2: 120 x 90 μm
  – TOUT, VSS, VDD: 90 x 90 μm
- Material: AlCu

8.1.6 Fail die identification

Every die is 100% electrically tested. Identification of dies which do not confirm with the electrical parameters is done by inking and wafer mapping.

Electronic wafer mapping (SECS II format) covers the electrical test results and additionally the results of mechanical/visual inspection.

See Ref. 2 “General specification for 8’’ wafer on UV-tape”.

8.1.7 Map file distribution

See Ref. 2 “General specification for 8’’ wafer on UV-tape”.

9. Functional description

9.1 Overview of transponder

Table 2. Overview of transponders

Parameter	Description	Unit
carrier frequency	125	kHz
coding read	Manchester/Biphase	-
coding write	Pulse duration	-
modulation	ASK (amplitude shift keying)	-
total memory size	256	bit
user memory read/write	128	bit
read only serial number	32	bit
data retention	10	year
data security	encryption, authentication, passwords	-
data integrity	half-duplex handshake, reverse data transmission	-

9.2 Memory map

The 256 bit memory area of the HITAG 2 transponder IC is divided into 8 pages. Each page has a size of 32 bits.

Depending on the operation mode (Crypto mode/Password mode) the memory is organized as described in the following:

page	content	access
0	Serial number	ro
1	Secret Key Low (32 bit)	r/w or 0
3	Secret Key High (16 bit) reserved Bit (14 bit)	r/w or ro
3	configuration (8 bit) password tag (24 bit)	r/w or ro
4	usable memory page	r/w or ro
5	usable memory page	r/w or ro
6	usable memory page	r/w or ro
7	usable memory page	r/w or ro

Fig 3. Memory map in Crypto Mode

page	content	access
0	Serial number	ro
1	password RWD	r/w or 0
2	reserved for future use	r/w or 0
3	configuration (8 bit) password tag (24 bit)	r/w or ro
4	usable memory page	r/w or ro
5	usable memory page	r/w or ro
6	usable memory page	r/w or ro
7	usable memory page	r/w or ro

Fig 4. Memory map in Password Mode

9.3 Definition of passwords and keys

Keys are cryptographic codes, which determine data encryption during data transfer between RWD and transponder IC. Keys are used to select a HITAG 2 transponder IC 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 RWD.

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 RWD.

Password TAG:	Password that the transponder sends to the RWD and which may be verified by the latter (depending on the configuration of the RWD).
Password RWD:	Password that the RWD 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 RWD and on the transponder have to be identical pairs.

Table 3. HITAG 2 in password mode

On the RWD		On the transponder
Password RWD	↔	Password RWD
as an option (depending on the configuration of the RWD):		
Password TAG	↔	Password TAG

Table 4. HITAG 2 in crypto mode

On the RWD		On the transponder
KEY LOW	↔	KEY LOW
KEY HIGH	↔	KEY HIGH
as an option (depending on the configuration of the RWD):		
Password TAG	↔	Password TAG

The passwords and keys are predefined by NXP 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" Section 9.4.3.3).

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

9.4 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 IC the Configuration Byte is read from the memory.

In case keys or passwords are changed, the transponder should be placed directly (0-distance) on the antenna of the RWD! In order to avoid any errors the transponder must not be moved during this write process. The programming should take place in a safe environment without electrical noise.

9.4.1 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. The 64 bits of the User Pages 4 and 5 are cyclically transmitted to the RWD.

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 RWD.

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 RWD.

9.4.2 Status flow

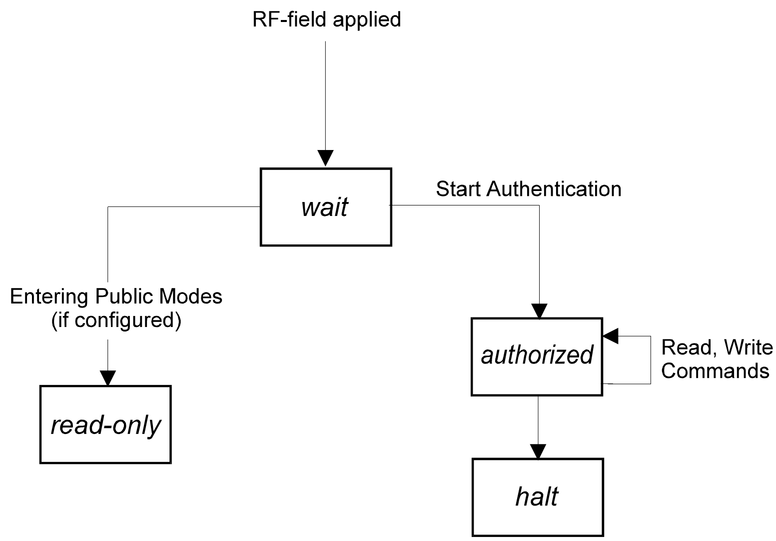


Fig 5. Status flow

After entering the RF-field the transponder enters the Wait Mode and 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 RWD.

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

9.4.3 Organization of the Configuration Byte

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

9.4.3.1 Configuration Byte

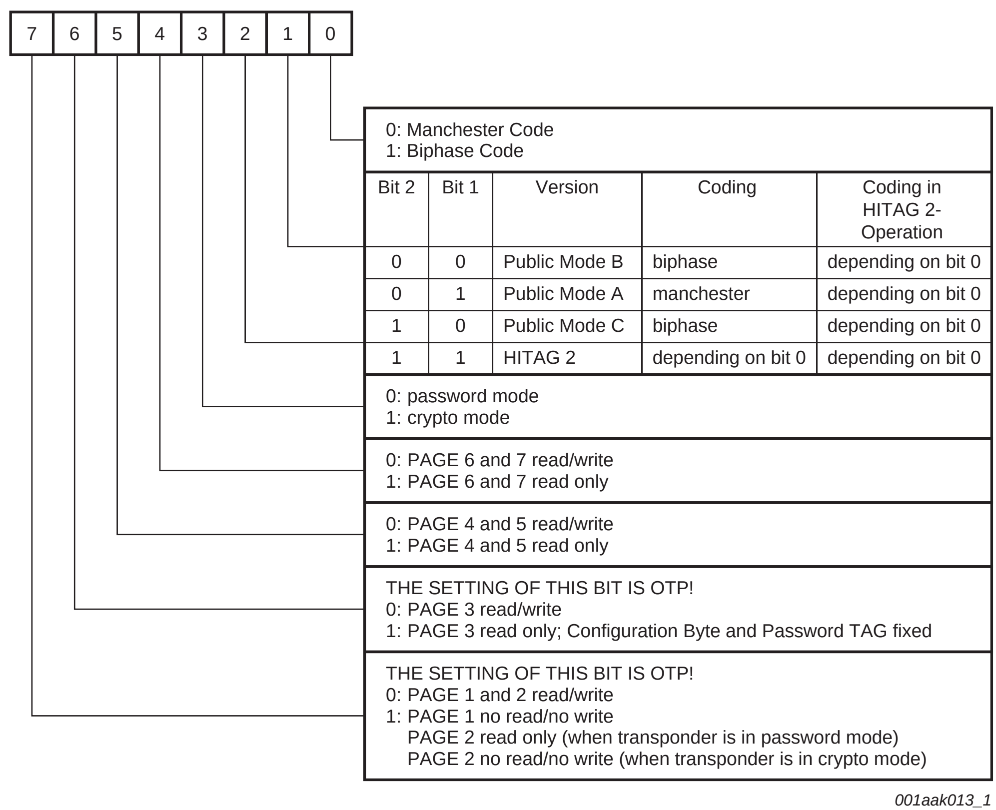


Fig 6. Configuration Byte

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.

9.4.3.2 Standard values of the Configuration Byte

Table 5. Standard values for the Configuration Byte

Mode	Value
Password Mode	06h
Crypto Mode	0Eh
Public Mode A	02h
Public Mode B	00h
Public Mode C	04h

9.4.3.3 Delivery configuration of HITAG 2 transponder IC

HITAG 2 transponder ICs are delivered with the following configuration by NXP Semiconductors:

Table 6. Delivery configuration

Unique serial number		
Serial number	read only	fixed
Configuration byte		
06h	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	4D 49 4B 52h (= “MIKR“)	
Password TAG	AA 48 54h	
Key Low	4D 49 4B 52h (= “MIKR“)	
Key High	4F 4Eh (= “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).

9.5 Electromagnetic characteristics

9.5.1 Magnetic flux densities

Since magnetic coupling is used for the data transmission between transponder and RWD the magnetic field is the most important attribute. Figure 7 shows the direction of the magnetic field lines with the transponder placed in the antenna field.

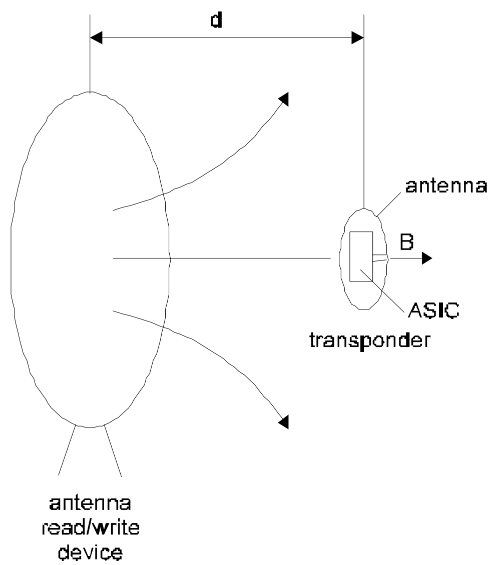


Fig 7. Magnetic coupling between RWD and transponder

9.5.2 Equivalent circuit for data and energy transfer

Figure 8 shows the model for the transmission channel realized as an inductive coupled circuit. The primary side (L1) represents the RWD antenna and the secondary side (L2) the antenna of the transponder.

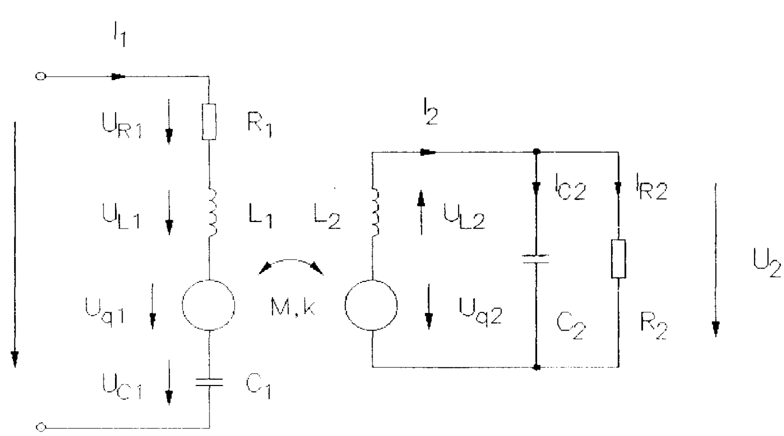


Fig 8. Equivalent circuit

9.6 Data transmission: transponder → RWD

9.6.1 Coding

Load modulation is used, when sending data to the RWD. 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:

Table 7. Coding and Bit length

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	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

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

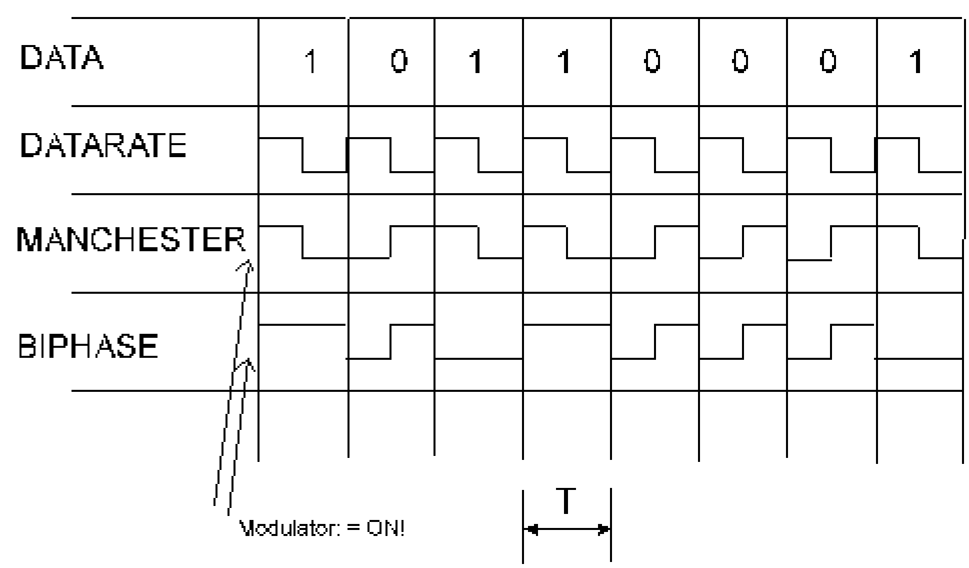


Fig 9. Data coding: Transponder → RWD

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

9.6.2 Modulation

Figure 10 shows the voltage at the antenna coil of the transponder. Measurement was done with an additional coil fixed at the transponder.

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

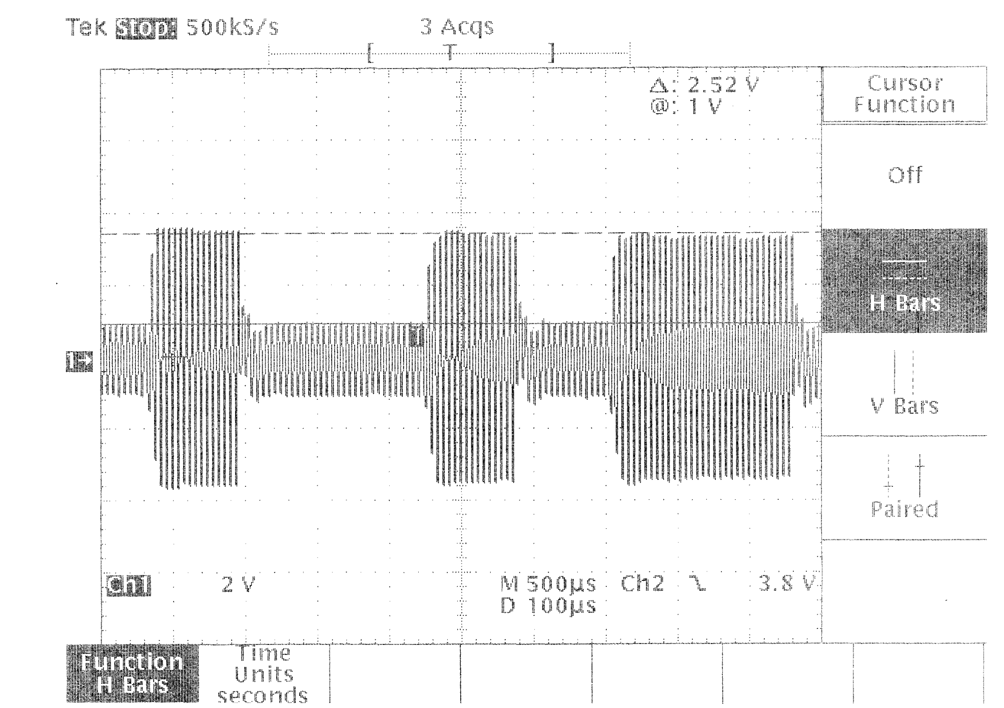


Fig 10. Transponder antenna coil voltage

9.7 Data transmission: RWD → transponder

9.7.1 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.

Figure 11 shows the data transmission from the RWD to the transponder.

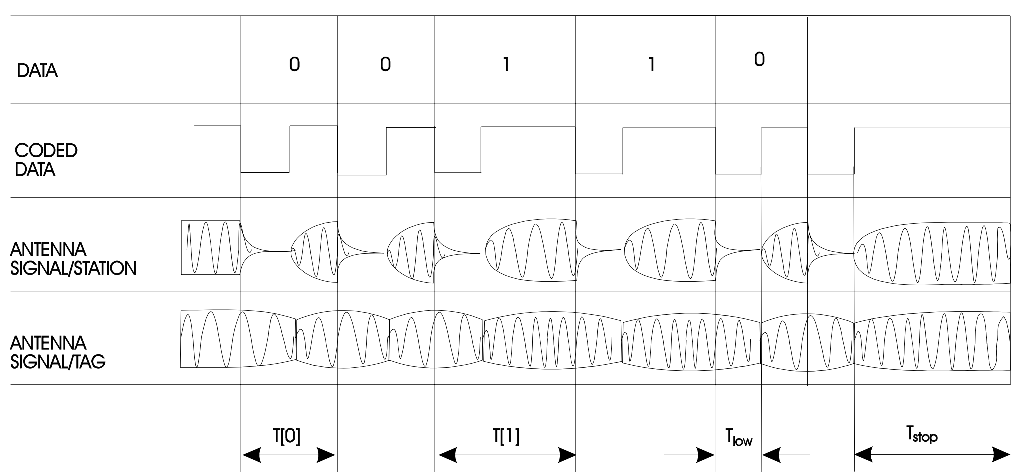


Fig 11. Data coding: RWD → transponder

Table 8. Timing values

Symbol	Description	Duration	Unit[2]
t_{low}	low field time	4 to 10	T_0[1]
T[0]	logic 0 pulse length	18 to 22	T_0
T[1]	logic 1 pulse length	26 to 32	T_0
t_{stop}	high field for stop condition	> 36	T_0

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

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

The average Bit rate from the RWD to transponder therefore is:

$$Bitrate = \frac{2}{T\lceil 0\rceil + T\lceil 1\rceil} = \ddot{5}, 2kB/s \qquad (1)$$

Remark: The end of each data sequence from RWD to transponder has to be a stop condition.

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

The following two examples show the timing for two RWDs.

Used timing values with a Proximity Reader Module are:

Table 9. Timing values with a Proximity Reader Module

Symbol	Description	Duration	Unit[1]
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

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

Used timing values with a Long Range Reader Module are:

Table 10. Timing values with a Long Reader Module

Symbol	Description	Duration	Unit[1]
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

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

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

9.7.2 Modulation

The following figure shows the antenna voltage of the RWD.

The minimum modulation depends on the quality factor of the antennas (transponder and RWD).

A recommended value for the quality factor of the RWD antenna is approx. 40.

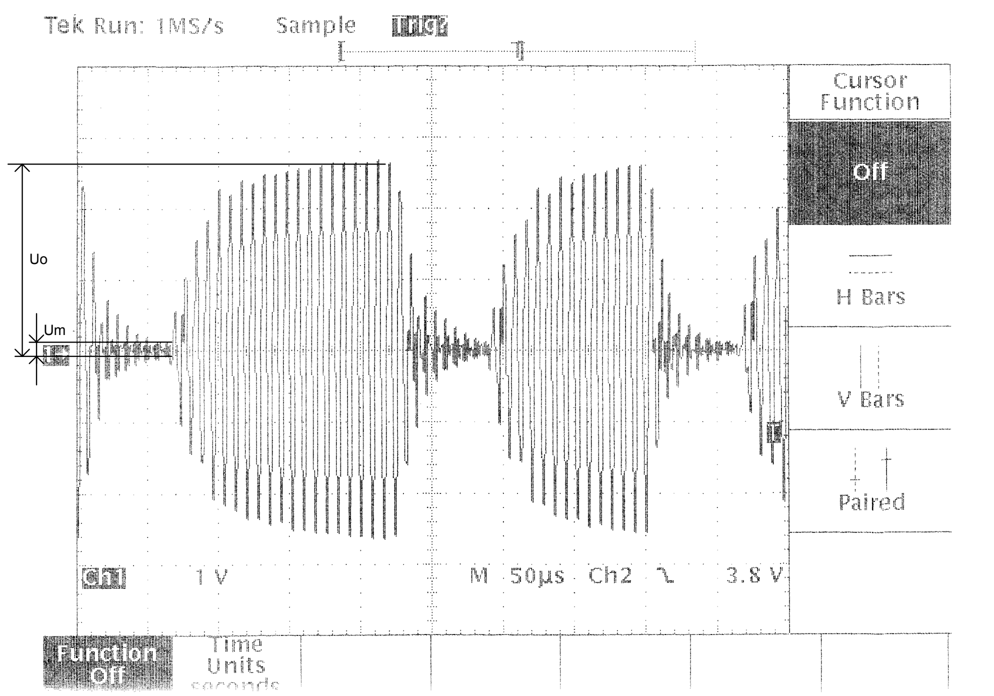


Fig 12. RWD antenna coil voltage

9.8 Switching the transmission direction

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

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

Table 11. t_{WAIT} times

Symbol	Description	Duration		Unit[2]
		Min	Max	
t_{WAIT1}	transponder switching from receive to transmit, wait time after end of data	199	206	T_0
t_{WAIT2}	transponder switching from transmit to receive, wait time after end of data	90[1]	-	T_0

[1] t_{WAIT2} must not exceed 5000 T_0!

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

9.8.1 Data integrity using the HITAG 2

For data transmission between RWD and transponders the HITAG 2 transponder IC 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 Section 10 “Command set and timing”

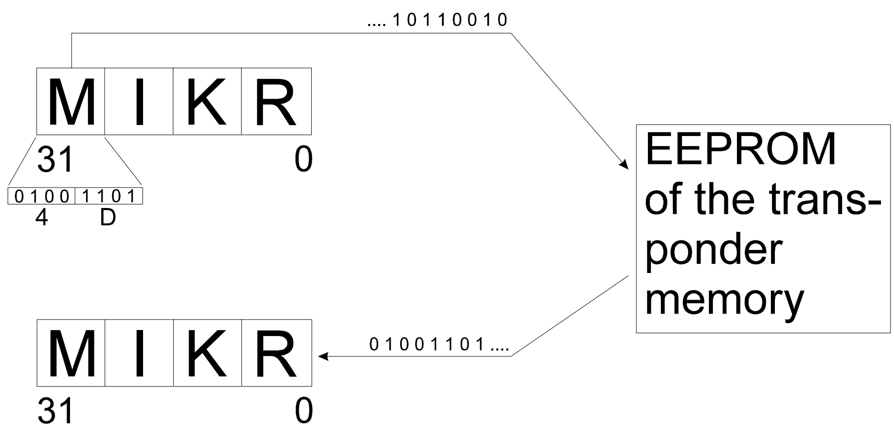
10. Command set and timing

There are two types of instructions

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

10.1 Data flow: RWD ↔ transponder

Please note that the transponder IC 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 RWD.

Fig 13. Data flow

10.2 START_AUTH-Instruction

Table 12. START_AUTH

CM1	CM0	ADDR4	ADDR3	ADDR2
1	1	0	0	0

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

10.2.1 Crypto Mode

After an instruction START_AUTH from the RWD all transponders in the field respond with a start sequence (5 bits ’1’) followed by their 32 bit serial number (SN).

RWD	11000	→		
Transponder		←	1 1 1 1 1	SN31 ....SN0
	↑ first in		start sequence	32 Bit serial number

RWD	32 bit PRN	32 bit secret data	→		
Transponder	first in		←	1 1 1 1 1	Config. Byte / Password TAG
					32 Bit

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

After the transponder has sent the serial number, the RWD 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 encrypted.

As the information about the configuration of the transponder (password or crypto) is transmitted with the configuration page, the RWD 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, when the memory supply is too low during the write operation.

Timing:

RWD		11000				PRN/PSW		
Transponder				ID number				Config Byte/Password TAG
	$t_{PowerUp}$	t_{START_AUTH}	t_{WAIT1}	t_{SN}	t_{WAIT2}	$t_{PZZ/SDS}$	t_{WAIT1}	t_{CONFIG}

Table 13. Timing in crypto mode

Symbol	Min	Typ	Max	Unit[1]
$t_{PowerUp}$	-	312.5	-	T_0
t_{START_AUTH}	-	116	-	T_0
t_{WAIT1}	199	-	206	T_0
t_{SN}	-	1184[2]	-	T_0
t_{WAIT2}	90	-	-	T_0
$t_{PZZ/SDS}$	1280	1536	1792	T_0
t_{CONFIG}	-	1184[2]	-	T_0
Total	-	**4630**	-	**T0**

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

[2] Timing defined by digital design and therefore fixed

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

10.2.2 Password Mode

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

RWD	11000 →				
Transponder		←	1 1 1 1 1	SN31 ....SN0
	↑ first in		start sequence	32 Bit serial number

RWD	32 bit PSW →			
Transponder	first in	←	1 1 1 1 1	Config. Byte / Password TAG
				32 Bit

The instruction START_AUTH cannot be repeated. A second START_AUTH resets the state-machine. Therefore the transponder only responds to every second START_AUTH.

After the transponder has sent the serial number, the RWD sends a 32 bit password. 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 RWD 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 memory 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:

RWD		11000				PSW		
Transponder				ID number				Config Byte/Password TAG
	$t_{PowerRUp}$	t_{START_AUTH}	t_{WAIT1}	t_{SN}	t_{WAIT2}	t_{PSW}	t_{WAIT1}	t_{CONFIG}

Table 14. Timing in password mode

Symbol	Min	Typ	Max	Unit[1]
$t_{PowerUp}$	-	312.5	-	T_0
t_{START_AUTH}	-	116	-	T_0
t_{WAIT1}	199	-	206	T_0
t_{SN}	-	1184[2]	-	T_0
t_{WAIT2}	90	-	-	T_0
$t_{PZZ/SDS}$	640	768	896	T_0
t_{CONFIG}	-	1184[2]	-	T_0
Total	-	**3860**	-	**T0**

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

[2] Timing defined by digital design and therefore fixed

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

10.2.3 Public Modes A and B

After the Configuration Byte is stored in the logic during power up, and after the synchronization phase of the state machine, the transponder waits for the instruction START_AUTH. If the RWD 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).

Table 15. Timings

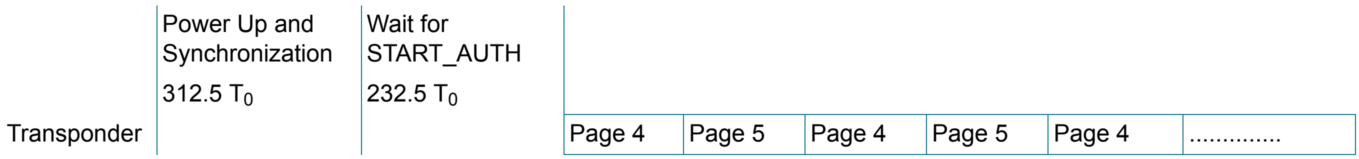
Symbol	Description	Duration	Unit[2]
$t_{PowerUp}$	internal power_up time	312.5	T_0
$t_{WAIT\ START\_AUTH}$	waiting time to receive the START_AUTH command	max. 232.5[1]	T_0

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

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

Public Mode A

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



Remark: As the RWD 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:

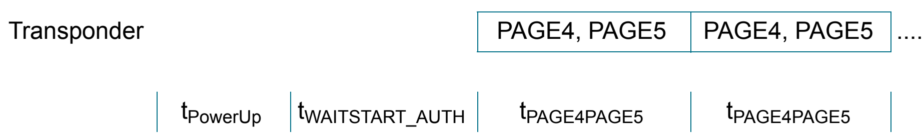


Table 16. Timing in Public Mode A

Symbol	Min	Typ	Max	Unit[1]
$t_{PowerUp}$	-	312.5	-	T_0
$t_{WAITSTART\_AUTH}$	-	-	232.5	T_0
$t_{PAGE4PAGE5}$	-	4096[2]	-	T_0
Total	-	**4640**	-	**T0**

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

[2] Timing defined by digital design and therefore fixed

If the RWD sends the instruction START_AUTH within the 232.5 T_0 after the power up the transponder behaves like a normal HITAG 2 transponder IC. 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 RWD without a start sequence as long as the transponder is in the field of the RWD. The data are transmitted in Biphase Code with a baudrate of 4 KBit/s.

	Power Up and Synchronization	Wait for START_AUTH						
	312.5 T_0	232.5 T_0						
Transponder			Page 4	Page 5	Page 6	Page 7	Page 4	....

If the RWD sends the instruction START_AUTH within the 232.5 T_0 after the power up the transponder behaves like a normal HITAG 2 transponder IC. Depending on bit 3 of the Configuration Byte, the communication is plain or encrypted.

Timing:

Transponder			PAGE4 .... PAGE5	.....
	$t_{PowerUp}$	$t_{WAITSTART\_AUTH}$	$t_{PAGE4...7}$	

Table 17. Timing in Public Mode B

Symbol	Min	Typ	Max	Unit[1]
$t_{PowerUp}$	-	312.5	-	T_0
$t_{WAITSTART\_AUTH}$	-	-	232.5	T_0
$t_{PAGE4...7}$	-	4096[2]	-	T_0
Total	-	**4640**	-	**T0**

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

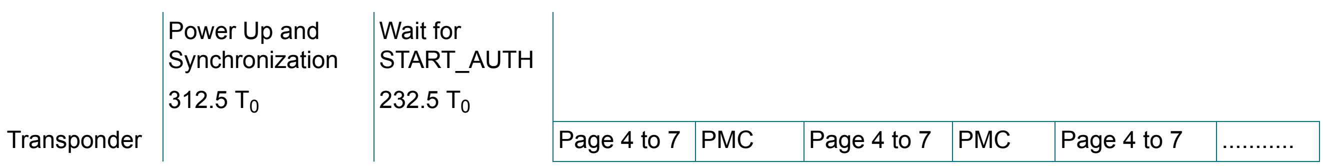
[2] Timing defined by digital design and therefore fixed

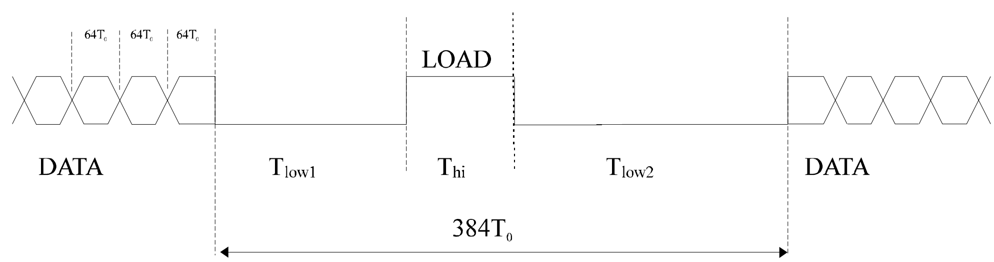
Public Mode C

With this additional feature a HITAG 2 transponder IC 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 synchronization phase of the state machine, the transponder waits for the instruction START_AUTH. If the RWD does not send the instruction START_AUTH within 232.5 T0 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 RWD without a start sequence as long as the transponder is in the field of the RWD. The data are transmitted in Biphase Code with a baudrate of 2 KBit/s. Between the 128 bit data blocks there is a Program Mode Check phase (PMC).





T_{hi} = 64 T_0

T_{low1} = 128 T_0

T_{low2} = 192 T_0

Fig 14. Program Mode check phase

If the RWD sends the instruction START_AUTH within the 232.5 T_0 after the power up the transponder behaves like a normal HITAG 2 transponder IC. Depending on bit 3 of the Configuration Byte, the communication is plain or encrypted.

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

Timing:

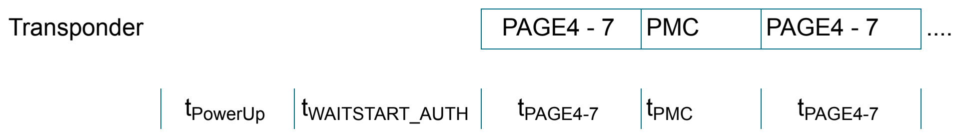


Table 18. Timing in Public Mode C

Symbol	Min	Typ	Max	Unit[1]
$t_{PowerUp}$	-	312.5	-	T_0
$t_{WAITSTART\_AUTH}$	-	-	232.5	T_0
$t_{PAGE4...7}$	-	8192[2]	-	T_0
t_{PMC}	-	384[2]	-	T_0
Total	-	**9120**	-	**T0**

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

[2] Timing defined by digital design and therefore fixed

10.3 Communication instructions

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

Table 19. Communication instructions

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 RWD to the transponder.

10.3.1 READ PAGE

RWD	1 1	ADDR (A4 .. A2)	0 0	inv. ADDR (/A4 .. /A2)	....	→
Transponder				←	1 1 1 1 1	32 Bit Data

↑
first out

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 RWD to transponder. To achieve a higher confidence 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:

RWD	Command			
Transponder			Data	
	t_{KOMM}	t_{WAIT1}	t_{DATA}	t_{WAIT2}

Table 20. Timing of READ PAGE instruction

Symbol	Min	Typ	Max	Unit[1]
t_{KOMM}	-	240	-	T_0
t_{WAIT1}	199	-	206	T_0
t_{DATA}	-	1184[2]	-	T_0
t_{WAIT2}	90	-	-	T_0
Total	-	**1750**	-	**T0**

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

[2] Timing defined by digital design and therefore fixed

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

10.3.2 READ PAGE INVERTED

RWD	0 1	ADDR (A4 .. A2)	1 0	inv. ADDR (/A4 .. /A2)	.... →
Transponder ←				1 1 1 1 1	32 Bit inverted Data

↑
first out

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 RWD to transponder. To achieve a higher confidence 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 RWD.

By alternating transmission of the instructions READ PAGE and READ PAGE INVERTED the data from the transponder to the RWD can be secured at a level that can be chosen by the user. Additionally check data can be stored in the transponder IC memory with the data.

Timing:

RWD	Command			
Transponder			Data	
	t_{KOMM}	t_{WAIT1}	t_{DATA}	t_{WAIT2}

Table 21. Timing of READ PAGE INVERTED instruction

Symbol	Min	Typ	Max	Unit[1]
t_{KOMM}	-	240	-	T_0
t_{WAIT1}	199	-	206	T_0
t_{DATA}	-	1184[2]	-	T_0
t_{WAIT2}	90	-	-	T_0
Total	-	**1750**	-	**T0**

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

[2] Timing defined by digital design and therefore fixed

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

10.3.3 WRITE PAGE

RWD

1 0	ADDR (A4 .. A2)	0 1	inv. ADDR (/A4 .. /A2)

.... →

↑

first out

Transponder

←

1 1 1 1 1	1 0	ADDR (A4...A2)	0 1	inv. ADDR (/A4 .. /A2)

RWD

32 Bit Data

The instruction WRITE 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 RWD to the transponder. To achieve a higher confidence level, this protocol can be repeated several times. The logic on the transponder checks if there is a failure in the sequence. The WRITE 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 an acknowledgement. This acknowledgement consists of the WRITE PAGE instruction and the page address in normal and inverted mode.

With this procedure the RWD knows, that the data are written to the correct address.

After the address sent from transponder to RWD has been checked, the RWD 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 PAGE command for a read-after-write has to be executed immediately following the WRITE PAGE command. If the memory 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:

RWD	Command				Data		
Transponder			Acknow.				
	t_{KOMM}	t_{WAIT1}	t_{QUIT}	t_{WAIT2}	t_{DATA}	t_{PROG}	t_{WAIT2}

Table 22. Timing WRITE PAGE instruction

Symbol	Min	Typ	Max	Unit[1]
t_{KOMM}	-	240	-	T_0
t_{WAIT1}	199	-	206	T_0
t_{QUIT}	-	480[2]	-	T_0
t_{WAIT2}	90	-	-	T_0
t_{DATA}	640	768	896	T_0
t_{PROG}	-	614[2]	-	T_0
t_{WAIT2}	90		-	T_0
Total	-	**2500**	-	**T0**

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

[2] Timing defined by digital design and therefore fixed

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

10.3.4 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 RWD. 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 RWD again. This means that the transponder has to leave the field of the antenna or the field has to be switched off (Reset).

RWD

0 0	ADDR (A4 .. A2)	1 1	inv. ADDR (/A4 .. /A2)	.... →

↑
first out

Transponder

←	1 1 1 1 1	0 0	ADDR (A4...A2)	1 1	inv. ADDR (/A4 .. /A2)

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 RWD to the transponder. To achieve a higher confidence 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:

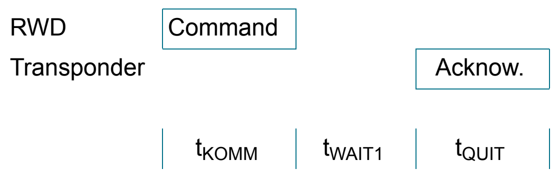


Table 23. Timing of HALT instruction

Symbol	Min	Typ	Max	Unit[1]
t_{KOMM}	-	240	-	T_0
t_{WAIT1}	199	-	1648	T_0
t_{QUIT}	-	480[2]	-	T_0
Total	-	**1000**	-	**T0**

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

[2] Timing defined by digital design and therefore fixed

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

10.4 Transponder coil specification - HT2MOA2S20

The HITAG 2 chip module has to be connected to a coil whose parameters are briefly described in the following.

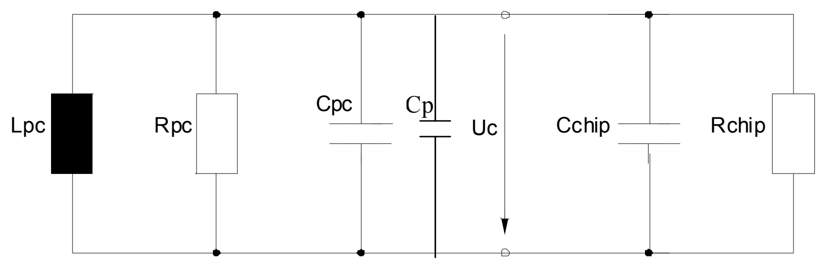


Fig 15. Equivalent circuit of the transponder

$$f_{res} = \frac{1}{2\pi\sqrt{(C_{chip} + C_{pc} + C_p)L_{pc}}} = 125kHz \rightarrow L_{pc} = \frac{1}{(2\pi f_{res})^2(C_{chip} + C_{pc} + C_p)} \quad (2)$$

	Description
U_c	voltage at the connection pads
f_{res}	resonant frequency of the transponder
L_{pc}	parallel inductivity of the coil (f = 125 kHz)
R_{pc}	parallel resistance of the coil (f = 125 kHz)
C_p	parasitic capacitance of the package
C_{chip}	210 pF ± 10 %
f_{resc}	self resonant frequency of the coil
R_{chip}	resistance of the chip
R_{pc}	> 45 kΩ ... to increase Q_{coil}
Q_{coil}	> 7.5 ... quality factor of transponder coil at 125 kHz
C_{pc}	parasitic capacitance of the coil
C_{chip}	capacitance of the chip (U_c > 4 Vpp)
L_{pc}	> 6.5 mH ... to ensure resonant frequency near 125 kHz

Remark: The parasitic capacitance of the package (C_p) must be considered.

Typical values for C_p molded tags: C_p = 6.0 pF

For a rough estimation (± 10 %) of the number of coil windings following formula can be used. It is assumed that the winding is done in circular form.

$$N = \sqrt[1,85]{\frac{L}{2U\ln\left(\frac{u}{d}\right)}} \tag{3}$$

Table 24. Abbreviations

	Description
N	number of windings
L	inductance [nH]
U	average coil circumference [cm]
d	copper diameter [mm]
u	average coil circumference [mm]

For fine tuning a measurement of the inductance and an according adjustment of the number of windings is necessary. This process always needs some iterations.

11. Limiting values

Table 25. Limiting values - HT2IC2002[1]

Symbol	Parameter	Conditions	Min	Max	Unit
V_{DD}	supply voltage		–0.5	+6.5	V
V_{ESD}	electrostatic discharge voltage	MIL-STD 883D, Method 3015.7, Human Body	2	-	kV
I_{lu}	latch-up current	MIL-STD 883D, Method 3023	100		mA
$I_{i(max)}$	maximum input current	IN1-IN2	–	30	mA_{peak}
Tj	junction temperature		–55	+140	°C

[1] Stresses above those listed under Absolute Maximum Ratings may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any conditions other than those described in the Operating Conditions and Electrical Characteristics section of this specification is not implied.

Table 26. Limiting values -HT2DC20S20 (SOT385-1)/ HT2MOA2S20 (SOT500-2)[1]

Symbol	Parameter	Conditions	Min	Max	Unit
T_{stg}	storage temperature		–55	+125	°C
	Magnetic flux density		–	0.2	T

[1] Stresses above those listed under Absolute Maximum Ratings may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any conditions other than those described in the Operating Conditions and Electrical Characteristics section of this specification is not implied.

12. Characteristics

Table 27. Electrical characteristics - HT2IC2002[1][2]

Symbol	Parameter	Conditions	Min	Max	Unit
Operating range					
T_A	Temperature	$R_{ThJunctionAmbient} \leq 30K/W$ @ I_{IN}=30mA	-40	85	°C
VDD	Supply Voltage		2.8	5.5	V
Power consumption					
I_{VDDQ}	Quiescent Current	VDD=3.5V, Limiter off	-	4	µA
I_{VDDI}	Idle Current	VDD=3.5V, V_{IN}=100mV @ 125 kHz, Limiter off	-	7	µA
Clock recovery					
V_{CLK}	Sensitivity	VDD=3.5V	-	100	mV
f_{CLK}	Frequency	V_{IN}=100mV, VDD=3.5V	-	250	kHz
Demodulator					
V_{DEMOD}	Sensitivity	V_{INHigh} - V_{INLow} @ V_{INHigh}=5Vp, T_0=8µs, T_{MOD}=6*T_0	-	2	V
T_{DEMOD}	Response Time	V_{INHigh}=5V, V_{INLow}=2.5V, T_0=8µs, T_{MOD}=6*T_0	4	24	µs
Modulator					
R_{IN1L}	R_IN1 linear	VDD=3.5V, V_{IN1}=0.5V, V_{IN2}=0V	1.6	3.0	kΩ
R_{IN1NL}	R_IN1 nonlinear	VDD=3.5V, V_{IN1}=1.5V, V_{IN2}=0V	480	1.46	kΩ
R_{IN2L}	R_IN2 linear	VDD=3.5V, V_{IN1}=0V, V_{IN2}=0.5V	3.4	6.4	kΩ
Voltage limiter					
$V_{LimitMin}$	Minimum Voltage	VDD @ I_{IN} ±10 µA	2.7	-	V
$V_{LimitMax}$	Maximum Voltage	VDD @ I_{IN} ±30 µA	-	5.5	V
Resonance capacitor					
$C_{ResInit}$		VDD=3.5V	189	231	pF
Power on reset					
V_{POR}	Static Power on Reset Level		1.3	2.3	V
VDD capacitor					
CVDD	VDD Capacitor Value	VDD=3.5V	0.9	2.0	nF
EEPROM characteristics					
	write current	VDD=2.8V	-	20	µA
	read current	VDD=2.8V	-	7	µA
t_{ret}	retention time	@ 55 °C	10	-	year
$N_{endu(W)}$	write endurance		100000	-	cycle

[1] In normal operation supply voltage is generated by on chip rectification and limitation of the AC voltage applied via antenna to pins IN1 and IN2, and can be measured at pins VDD and VSS.

[2] Pins VDD and VSS are not connected for normal operation but can be used for forcing supply voltages during test.

Table 28. Electrical characteristics - HT2DC20S20 (SOT385-1)

Symbol	Parameter	Conditions	Min	Max	Unit
T_A	ambient temperature	RThJunctionAmbient ≤ 30 K/W @ IINpeak = 30 mA	–25	85	°C
f_{RES}	resonance frequency		121	129	kHz
B_W	bandwidth		2.3	-	kHz
B_{thr}	magnetic flux density, data transmission from transponder to base station	f_0 = 125 kHz	35	400[1]	μT_{pp}
B_{prog}	magnetic flux density for programming the EEPROM	m = 0.95 f_0 = 125 kHz $t_{low} = 8T_0$	35	400[1]	μT_{pp}
B_{auth}	magnetic flux density for mutual authentication	m = 0.95 f_0 = 125 kHz tlow = $8T_0$	35	400[1]	μT_{pp}
B_{read}	field absorption due to the modulation of the transponder	f_0 = 125 kHz $B_{field} = 35\ \mu T_{pp}$	8	-	μT_{pp}
Mi_{PRG}	modulation index (m) of the base station for programming and authentication	$B_{field} = 35\ \mu T_{pp}$ f_0 = 125 kHz $t_{low} = 8T_0$	95	100	%

[1] Maximum available field strength of the test equipment. Transponder limit has not been characterized.

All parameters are characterized with the Scemtec test equipment (STM-1), available from SCEMTEC, Reichshof-Wenrath,Germany.

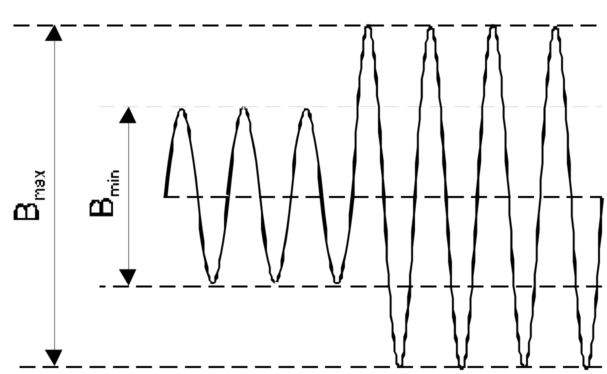


Fig 16. Modulation index

$$m = \frac{(B_{max} - B_{min})}{(B_{max} + B_{min})} \tag{4}$$

$$B_{read} = |B_{max} - B_{min}| \tag{5}$$

Table 29. Electrical characteristics - HT2MOA2S20 (SOT500-2)

Symbol	Parameter	Conditions	Min	Max	Unit
Operating range					
T_A	ambient temperature	$R_{ThJunctionAmbient} \leq 30$ K/W @ $I_{INpeak} = 30$ mA	–25	85	°C
$V_{IN, TH}$	input threshold voltage	start modulation after SETCC	-	3.9	V_p
$V_{IN, RD}$	input read voltage	read EEPROM	-	4.5	V_p
$V_{IN, WR}$	input write voltage	write EEPROM	-	4.7	V_p
Modulator					
R_{MODL}	R_MOD linear	$V_{INLow} \leq 2.0\ V_p$	-	4.0	kΩ
R_{MODNL}	R_MOD linear	$V_{INLow} \leq 2.0\ V_p$	-	3.6	kΩ
Resonance capacitor					
	$C_{RESInit}$	$V_{IN} = 4.0\ V_p$	189	231	pF

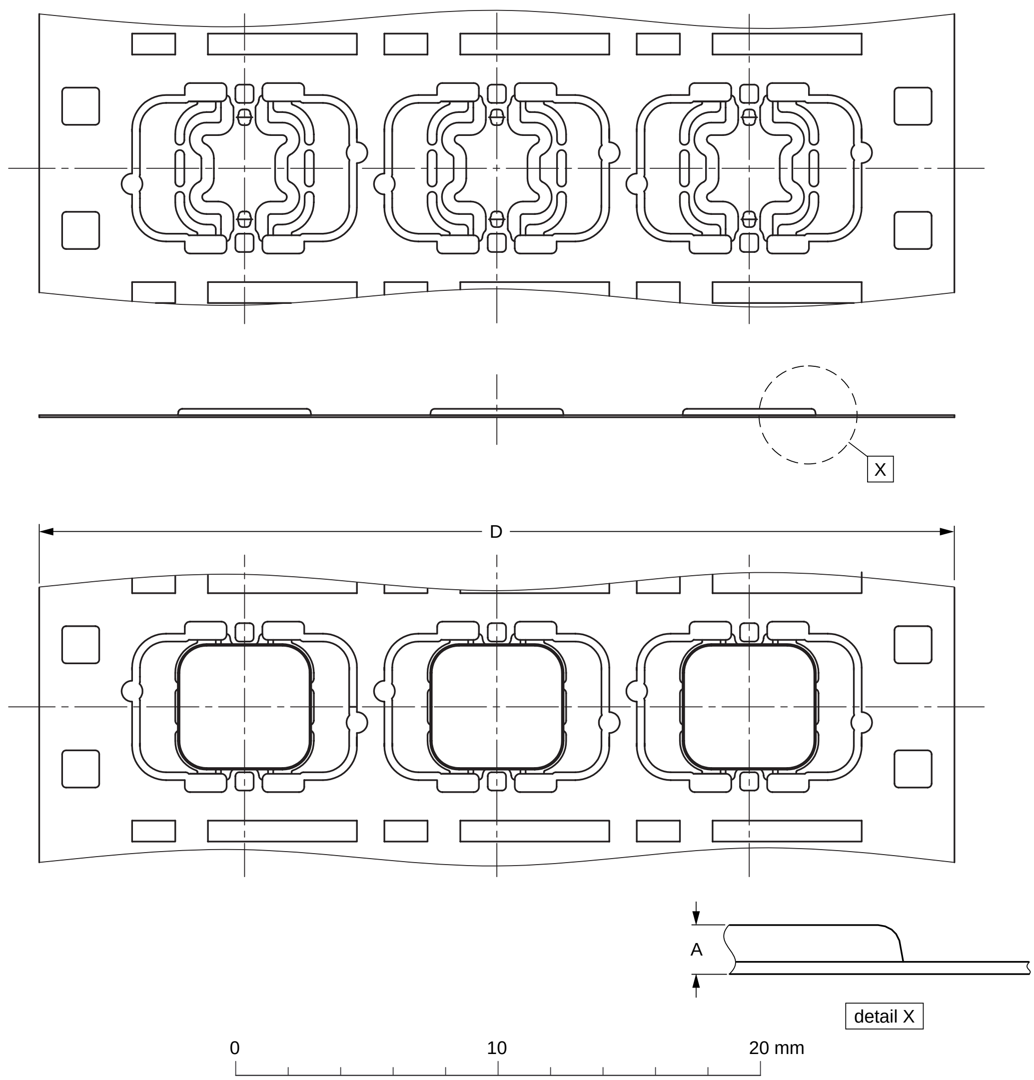
13. Mechanical characteristics

Table 30. Mechanical characteristics HT2DC20S20 (SOT385-1)

Parameter	Value	Unit
Mechanical dimensions	12 x 6 x 3	mm
Protection class	IP67	
Casting material	epoxy resin	
Housing color	black	
Vibration • 20 to 200 Hz • 3-axis • IEC 68-2-6, Test Fc	20	g

14. Package outline

PLLMC: plastic leadless module carrier package; 35 mm wide tape **SOT500-2**



DIMENSIONS (mm are the original dimensions)

UNIT	A (1) max.	D	
mm	0.33	35.05 34.95	For unspecified dimensions see PLLMC-drawing given in the subpackage code.

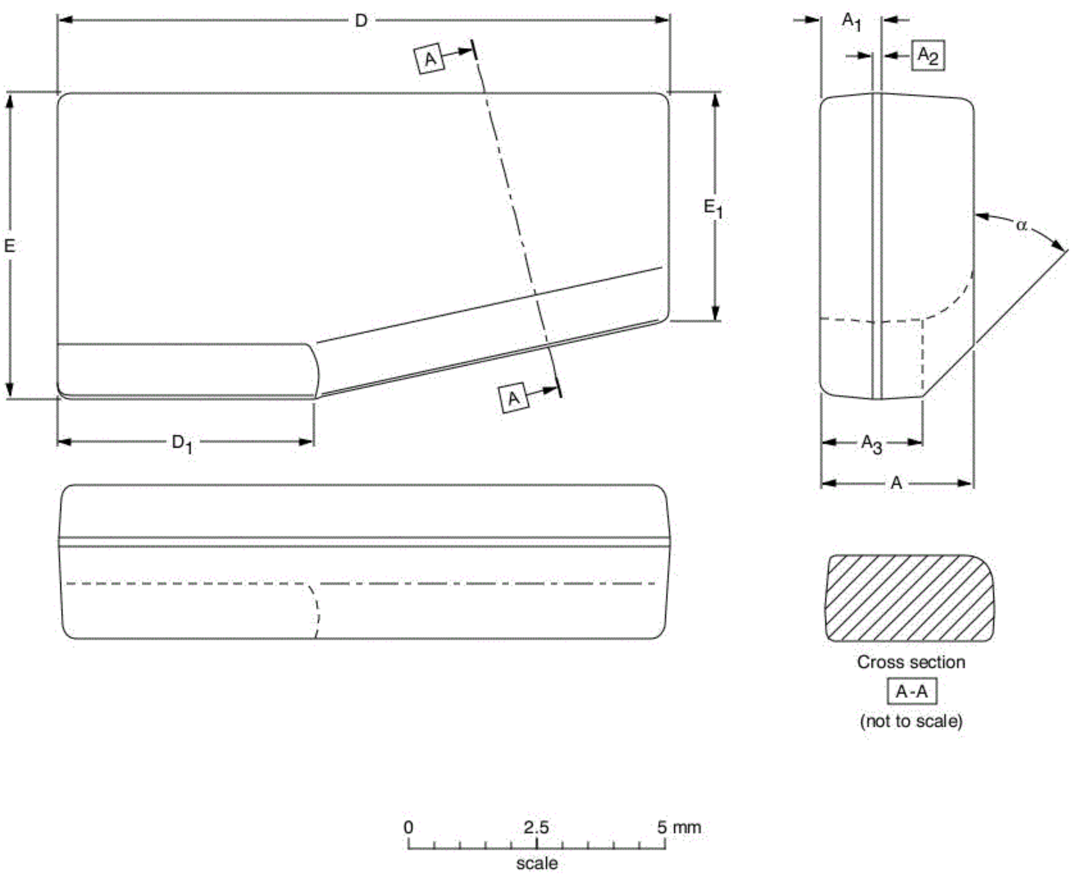
Note

1. Total package thickness, exclusive punching burr.

OUTLINE VERSION	REFERENCES				EUROPEAN PROJECTION	ISSUE DATE
	IEC	JEDEC	JEITA			
SOT500-2	- - -	- - -	- - -			~~03-09-17~~ 06-05-22

Fig 17. Package outline SOT500-2 (HT2DCS20)

PLLMC: plastic leadless module carrier package **SOT385-1**



DIMENSIONS (mm are the original dimensions)

UNIT	A	A_1	A_2	A_3	$D^{(1)}$	$D_1^{(1)}$	$E^{(1)}$	$E_1^{(1)}$	α
mm	3.05 2.90	1.2 1.1	0.165	2.1 1.9	12.1 11.9	5.1 4.9	6.1 5.9	4.6 4.4	46° 44°

Note

1. Plastic protrusions of 0.2 mm per side are not included.

OUTLINE VERSION	REFERENCES				EUROPEAN PROJECTION	ISSUE DATE
	IEC	JEDEC	JEITA			
SOT385-1						~~03-03-12~~ 03-09-23

Fig 18. Package outline SOT385-1 (HT2MOA2S20)

15. Abbreviations

Table 31. Abbreviations

Abbreviation	Definition
AC	Anticollision Code
BPLM	Binary Pulse Length Modulation
CRC	Cyclic Redundancy Check
EEPROM	Electrically Erasable Programmable Memory
IC	Integrated Circuit
RO	Read Only
R/W	Read/Write
RWD	Read Write Device
SN	Serial Number
WO	Write Only

16. References

[1] **Application note —** AN10214, HITAG Coil Design Guide, Transponder IC BL-ID Doc.No.: 0814**[1]

[2] **General specification for 8” wafer on UV-tape —** Delivery type description, BL-ID Doc.No.: 1005**[1]

1. ** ... document version number

17. Revision history

Table 32. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
188330	20100226	Product data sheet	-	-

18. Legal information

18.1 Data sheet status

Document status[1][2]	Product status[3]	Definition
Objective [short] data sheet	Development	This document contains data from the objective specification for product development.
Preliminary [short] data sheet	Qualification	This document contains data from the preliminary specification.
Product [short] data sheet	Production	This document contains the product specification.

[1] Please consult the most recently issued document before initiating or completing a design.

[2] The term ‘short data sheet’ is explained in section “Definitions”.

[3] The product status of device(s) described in this document may have changed since this document was published and may differ in case of multiple devices. The latest product status information is available on the Internet at URL http://www.nxp.com.

18.2 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

Short data sheet — A short data sheet is an extract from a full data sheet with the same product type number(s) and title. A short data sheet is intended for quick reference only and should not be relied upon to contain detailed and full information. For detailed and full information see the relevant full data sheet, which is available on request via the local NXP Semiconductors sales office. In case of any inconsistency or conflict with the short data sheet, the full data sheet shall prevail.

Product specification — The information and data provided in a Product data sheet shall define the specification of the product as agreed between NXP Semiconductors and its customer, unless NXP Semiconductors and customer have explicitly agreed otherwise in writing. In no event however, shall an agreement be valid in which the NXP Semiconductors product is deemed to offer functions and qualities beyond those described in the Product data sheet.

18.3 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors’ aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the *Terms and conditions of commercial sale* of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in medical, military, aircraft, space or life support equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors accepts no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer’s own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on a weakness or default in the customer application/use or the application/use of customer’s third party customer(s) (hereinafter both referred to as “Application”). It is customer’s sole responsibility to check whether the NXP Semiconductors product is suitable and fit for the Application planned. Customer has to do all necessary testing for the Application in order to avoid a default of the Application and the product. NXP Semiconductors does not accept any liability in this respect.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer’s general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from national authorities.

Quick reference data — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

Non-automotive qualified products — Unless the data sheet of an NXP Semiconductors product expressly states that the product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

18.4 Licenses

ICs with HITAG functionality

NXP Semiconductors owns a worldwide perpetual license for the patents US 5214409, US 5499017, US 5235326 and for any foreign counterparts or equivalents of these patents. The license is granted for the Field-of-Use covering: (a) all non-animal applications, and (b) any application for animals raised for human consumption (including but not limited to dairy animals), including without limitation livestock and fish.

Please note that the license does not include rights outside the specified Field-of-Use, and that NXP Semiconductors does not provide indemnity for the foregoing patents outside the Field-of-Use.

18.5 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

HITAG — is a trademark of NXP B.V.

19. Contact information

For more information, please visit: **http://www.nxp.com**

For sales office addresses, please send an email to: **salesaddresses@nxp.com**

20. Tables

21. Figures

22. Contents

Date of release: 26 February 2010 188330
Document identifier: 188330