DATA SHEET

HITAG S

HTS IC H32/HTS IC H56/HTS IC H48

Transponder IC

Functional Specification

Objective Specification

Revision 1.1

Confidential

October 2002

Philips

Semiconductors

PHILIPS

CONTENTS

1 FEATURES..5
1.1 Protocol..5
1.2 Memory..5
1.3 Supported Standards..5
1.4 Security Features..5
1.5 Delivery Types..5
2 GENERAL DESCRIPTION..6
2.1 Target Markets:..6
2.2 Customer Application Support and Training..7
3 BLOCKDIAGRAM..8
4 ORDERING INFORMATION..9
5 REFERENCE DOCUMENTS..9
6 MEMORY ORGANISATION..10
6.1 Unique Identifier (UID)..11
6.2 HITAG S Plain Mode..11
6.3 HITAG S Authentication Mode..12
7 FUNCTIONAL DESCRIPTION..13
7.1 Basic System Configuration..13
7.2 Energy Transmission..13
7.3 Data Transmission: Transponder → Read/Write Device..14
7.3.1 Coding..14
7.3.2 Data Rate..15
7.4 Data Transmission: Read/Write Device → Transponder..15
7.4.1 Coding..15
7.4.2 Modulation details..17
8 CONFIGURATION..18
8.1 Configuration Page..18
8.2 Delivery Configuration..21
8.2.1 HITAG S32..21
8.2.2 HITAG S256..21
8.2.3 HITAG S2048..22
9 PROTOCOL TIMING..23

9.1 HITAG S Transponder Start up Time ... 23
9.2 HITAG S Transponder Reset Time ... 23
9.3 HITAG S Transponder waiting time before transmitting a response after receiving an EOF ... 24
9.4 HITAG S Transponder programming time ... 24
9.5 HITAG S Transponder waiting time before transmitting data in TTF Mode ... 25
9.6 HITAG S Transponder Mode switching window ... 25
9.7 Read/Write Device waiting time before sending a subsequent command ... 26

10 STATE DIAGRAM ... 27
10.1 General description of states ... 27
10.2 HITAG S32 ... 28
10.3 HITAG S256 and HITAG S2048 ... 29

11 COMMAND SET ... 30
11.1 General Comments ... 30
11.2 UID REQUEST xx ... 30
11.3 AC SEQUENCE ... 31
11.4 SELECT (UID) ... 31
11.5 CHALLENGE ... 32
11.6 SELECT_QUIET (UID) ... 33
11.7 READ PAGE ... 33
11.8 READ BLOCK ... 34
11.9 WRITE PAGE ... 34
11.10 WRITE BLOCK ... 35
11.11 QUIET ... 36

12 TRANSPONDER TALKS FIRST (TTF) MODE ... 37
12.1 32 Bit TTF Mode ... 37
12.2 64 Bit TTF Mode ... 38
12.3 128 Bit TTF Mode ... 38

13 DATA INTEGRITY / CALCULATION OF CRC ... 39
13.1 Data Transmission: Read/Write Device to HITAG S Transponder ... 39
13.2 Data Transmission: HITAG S Transponder to Read/Write Device ... 39
13.2.1 Standard Response Protocol Mode ... 39
13.2.2 Advanced/Fast Advanced Response Protocol Mode ... 39
13.3 Source Code for CRC-Checksum ... 40

14 ABBREVIATIONS ... 41

15 DEFINITIONS 42

16 DISCLAIMERS.. 42

16.1 Life support applications 42

17 REVISION HISTORY.. 43

1 FEATURES

Integrated Circuit for Contactless Identification Transponders and Cards

Integrated resonance capacitor of 210 pF with +/- 5 % tolerance over full production.

Frequency range 100..150 kHz.

1.1 Protocol

Modulation Read/Write Device → Transponder: 100 % ASK and Binary Pulse Length Coding

Modulation Transponder → Read/Write Device: Strong ASK modulation with Anticollision, Manchester and Biphase Coding

Data integrity check (CRC)

Optional Transponder Talks First Modes with user defined data length

Temporary switch from Transponder Talks First into Reader Talks First Mode

Data Rate Read/Write Device to Transponder: 5.2 kBit/s

Data Rates Transponder to Read/Write Device: 2 kBit/s, 4 kBit/s, 8 kBit/s

1.2 Memory

Three memory options (32 Bit UID, 256 Bit, 2048 Bit)

More than 100 000 erase/write cycles

10 years non - volatile data retention

Secure Memory Lock functionality

1.3 Supported Standards

ISO 11784/85, ISO 14223/1 compliant

Compliant to German Waste Management Standard (BDE)

Compliant to German Pigeon Race Standard

1.4 Security Features

32 Bit Unique Identification Number (UID)

48 Bit secret key based encrypted authentication

1.5 Delivery Types

Sawn, gold - bumped 8 inch Wafer

Contactless Chip Card Module MOA2

I – Connect (Low Cost Flip Chip Package)

2 GENERAL DESCRIPTION

The HITAG™ product line is well known and established in the contactless identification market.

Due to the open marketing strategy of Philips Semiconductors there are various manufacturers available for both the transponders / cards as well as the Read/Write Devices. All of them supporting HITAG 1 and HITAG 2 transponder IC's. With the new HITAG S family, this existing infrastructure is extended with the next generation of IC's being substantially smaller in mechanical size, lower in cost, offering more operation distance and speed, but still being operated with the same reader infrastructure and transponder manufacturing equipment.

One Protocol - three memory options.

The protocol and command structure for HITAG S is based on HITAG 1, including anticollision algorithm.

Three different memory sizes are offered and can be operated using exactly the same protocol.

HITAG S 32	32 Bit Unique Identifier	Read Only
HITAG S 256	256 Bit Total Memory	Read/Write
HITAG S 2048	2048 Bit Total Memory	Read/Write

2.1 Target Markets:

Animal Identification
Basically, the animal id market can be divided into two different areas:

a) Identification of pet animals

Some countries require that the your dog/cat is being microchiped prior to immigration.
But it is also of advantage in case your pet is getting lost. The microchiped pet gets easily identified with a handheld reader and thus can be distinguished from stray animals.

The ISO standard 11784/85 is well established in this markets and HITAG S256 and HITAG S2048 are compliant to this standard, while offering additional memory for storage of customised off line data, such as Phone Number/Address of the pets owner.

b) Identification and Tracking of livestock like cattle, pork and sheep.

Also in this markets the ISO standard 11784/85 is playing a major role.

Laundry Automation

- Identify 200 pcs of garment with one Read/Write Device
- Long operation distance with typical small shaped laundry button transponders
- Insensitive to harsh conditions like pressure, heat and water.

Beer Keg and Gas Cylinder Logistic

- Recognising a complete pallet of gas cylinders at one time.
- Long writing distance.
- Voluntarily change between TTF Mode with user defined data length and Read/Write Modes with out changing the configuration on the transponder.
- Authenticity check at the Beer pubs- between beer bumper and supplied beer keg, provides a safe protection of the beer brand.

Pigeon Race Sports

According to European pigeon race standards, offering the additional shadow memory, that is required in some European companies.

Security Applications

Authenticity check for high level brands or for original refilling e.g. toner for fax machines.

Access Control, Company Cards, Amusement parks

The included encrypted authentication feature is well suited for applications like access control and vending machines. In particular the combined application with one company card opening the barrier for the car parking, opening the access to the building and rooms with different security levels, offering drinks and coffee from the vending machines in the socialising area.

2.2 Customer Application Support and Training

Within the dedicated CAS team within the BU Identification.

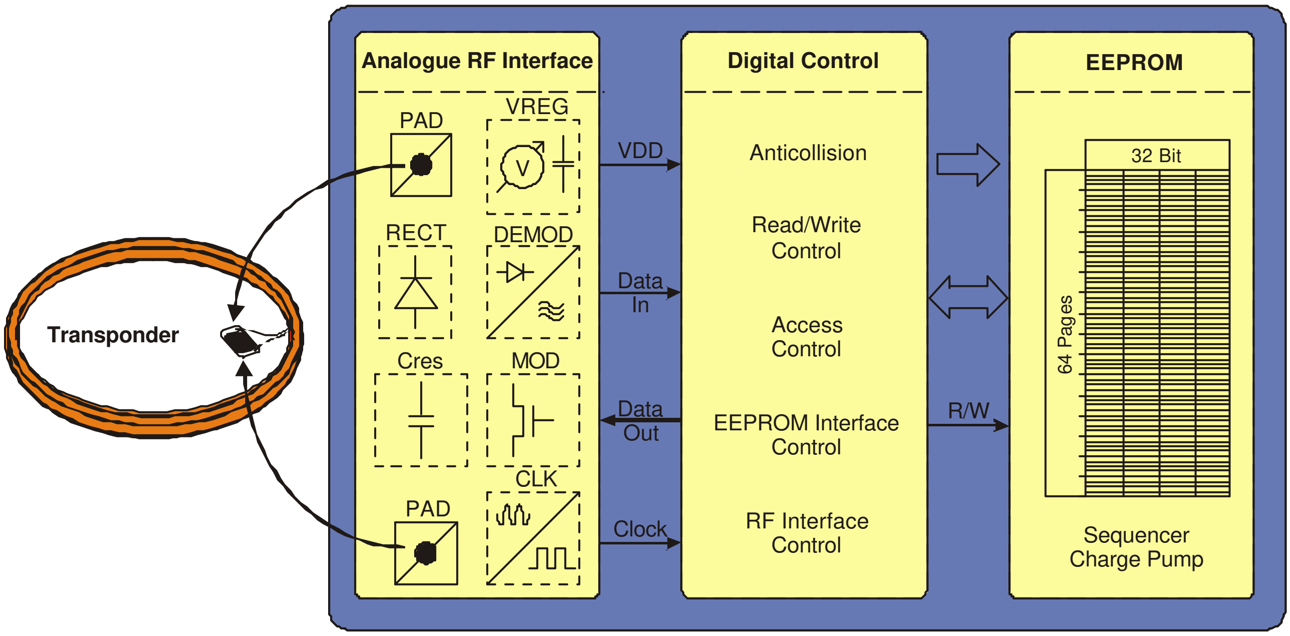
Please Contact:

info.bli@philips.com

Accompanying Data Sheets and Application Notes:

http://www.semiconductors.com/markets/identification/customer/download/index.html#hitag

3 BLOCKDIAGRAM



The HITAG S Transponder requires no internal power supply. The contactless interface generates the power supply and the system clock via the resonant circuitry by inductive coupling to the Read/Write Device (RWD). The interface also demodulates data that are transmitted from the RWD to the HITAG S Transponder, and modulates the magnetic field for data transmission from the HITAG S Transponder to the RWD.

Data are stored in a non-volatile memory (EEPROM). The EEPROM has a memory capacity up to 2048 Bit and is organised in 64 Pages consisting of 4 Bytes each (1 Page = 32 Bits).

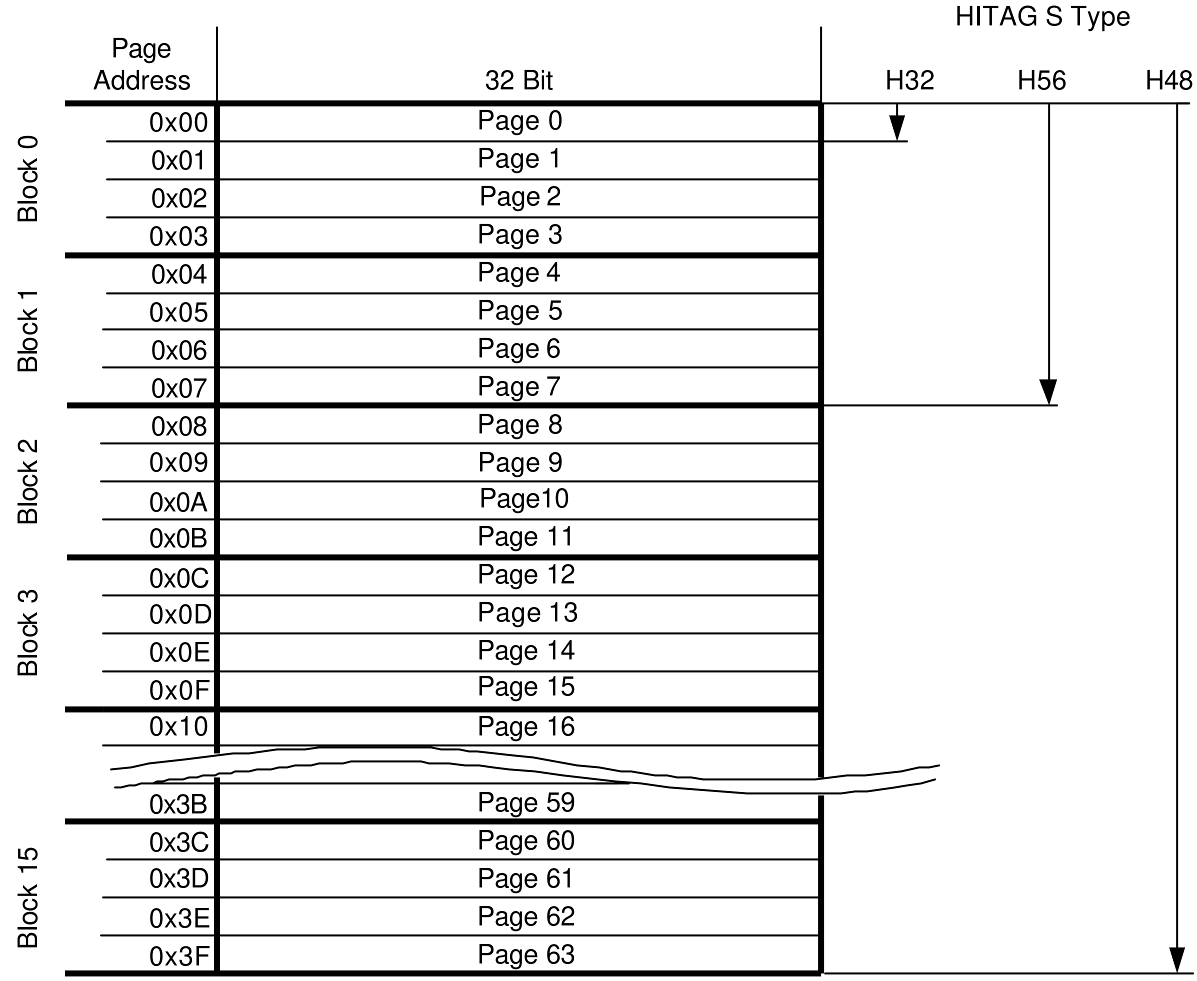
4 ORDERING INFORMATION

Type Name	Memory Size	Description	Ordering Code
HTS IC H**32** 01DW/V4	**32** Bit	Sawn 8" wafer on foil (FFC), 150 µm, inked and mapped, with gold bumps	xxxx xxx xxxxx
HTS IC H**56** 01DW/V4	2**56** Bit	Sawn 8" wafer on foil (FFC), 150 µm, inked and mapped, with gold bumps	
HTS IC H**48** 01DW/V4	20**48** Bit	Sawn 8" wafer on foil (FFC), 150 µm, inked and mapped, with gold bumps	
HTS MO H**32** 01DV	**32** Bit	MOA2 Package	
HTS MO H**56** 01DV	2**56** Bit	MOA2 Package	
HTS MO H**48** 01DV	20**48** Bit	MOA2 Package	
HTS FC H**32** 01DV/VH	**32** Bit	Flip Chip Package, Hot Laminated	
HTS FC H**56** 01DV/VH	2**56** Bit	Flip Chip Package, Hot Laminated	
HTS FC H**48** 01DV/VH	20**48** Bit	Flip Chip Package, Hot Laminated	

5 REFERENCE DOCUMENTS

- General Quality Specification
- General Specification for 8" Wafer
- Bumped Wafer Specification
- Addendum Bumped Wafer Specification HTS IC H32/ HTS IC H56/ HTS IC H48
- Contactless Chip Card Module Specification
- Addendum Contactless Chip Card Module Specification HTS MO H32/HTS MO H56/HTS MO H48
- Flip Chip Package Specification FCP 2.1
- Addendum Flip Chip Package Specification HTS FC H32/HTS FC H56/HTS FC H48

6 MEMORY ORGANISATION



The EEPROM has a memory capacity up to 2048 Bit and is organised in 16 Blocks consisting of 4 Pages each for commands with Block access. A Page consists of 4 Bytes each (1 Page = 32 Bits) and is the smallest access unit.

Addressing is done Page by Page (Page 0 up to 63) and access is gained either Page by Page or Block by Block entering the respective Page start address. In case of Block Read/Write access, the transponder is processed from the start Page address within one block to the end of the corresponding block.

Three different types of HITAG S IC’s with different memory sizes as shown in the figure above are available.

6.1 Unique Identifier (UID)

Page 0 contains the 32 Bit Unique Identifier (UID) which is programmed during the manufacturing process. Page 0 access: Read Only (RO)

	MSByte			LSByte
Page Address	MSB LSB	MSB LSB	MSB LSB	MSB LSB
0x00	UID 3	UID 2	UID 1	UID 0

6.2 HITAG S Plain Mode

Page 1:

In Plain Mode, Page 1 contains three configuration Bytes CON 0 to CON 2 and a reserved byte.

	MSByte			LSByte
Page Address	MSB LSB	MSB LSB	MSB LSB	MSB LSB
0x01	Reserved	CON 2	CON 1	CON 0

Page 2 - 63:

In Plain Mode, Pages 2 – 63 can be used to store user data.

	MSByte			LSByte
Page Address	MSB LSB	MSB LSB	MSB LSB	MSB LSB
0x02 – 0x3F	Data 3	Data 2	Data 1	Data 0

Memory Map for HITAG S in Plain Mode:

	MSByte			LSByte
Page Address	MSB LSB	MSB LSB	MSB LSB	MSB LSB
0x00	UID 3	UID 2	UID 1	UID 0
0x01	Reserved	CON 2	CON 1	CON 0
0x02	Data 3	Data 2	Data 1	Data 0
0x03	Data 3	Data 2	Data 1	Data 0

6.3 HITAG S Authentication Mode

Page 1:

In Authentication Mode, Page 1 contains three configuration Bytes CON 0 to CON 2 and the password high Byte PWDH 0.

	MSByte			LSByte
Page Address	MSB LSB	MSB LSB	MSB LSB	MSB LSB
0x01	PWDH 0	CON 2	CON 1	CON 0

Page 2:

In Authentication Mode, Page 2 contains the password low Bytes PWDL 0 and PWDL 1 and the key high Bytes KEYH 0 and KEYH 1.

	MSByte			LSByte
Page Address	MSB LSB	MSB LSB	MSB LSB	MSB LSB
0x02	KEYH 1	KEYH 0	PWDL 1	PWDL 0

Page 3:

In Authentication Mode, Page 3 contains the key low Bytes KEYL 0 - KEYL 3.

	MSByte			LSByte
Page Address	MSB LSB	MSB LSB	MSB LSB	MSB LSB
0x03	KEYL 3	KEYL 2	KEYL 1	KEYL 0

Page 4 - 63:

In Authentication Mode, Pages 4 – 63 can be used to store user data.

	MSByte			LSByte
Page Address	MSB LSB	MSB LSB	MSB LSB	MSB LSB
0x04 – 0x3F	Data 3	Data 2	Data 1	Data 0

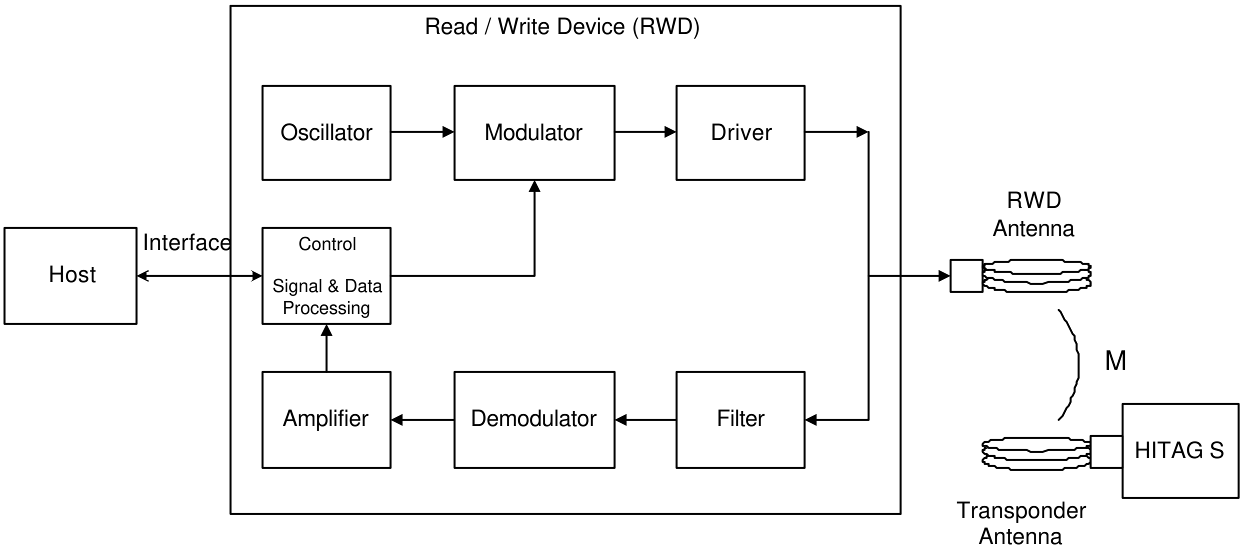
Memory Map for HITAG S in Authentication Mode:

	MSByte			LSByte
Page Address	MSB LSB	MSB LSB	MSB LSB	MSB LSB
0x00	UID 3	UID 2	UID 1	UID 0
0x01	PWDH 0	CON 2	CON 1	CON 0
0x02	KEYH 1	KEYH 0	PWDL 1	PWDL 0
0x03	KEYL 3	KEYL 2	KEYL 1	KEYL 0
0x04	Data 3	Data 2	Data 1	Data 0
0x05	Data 3	Data 2	Data 1	Data 0

7 FUNCTIONAL DESCRIPTION

7.1 Basic System Configuration

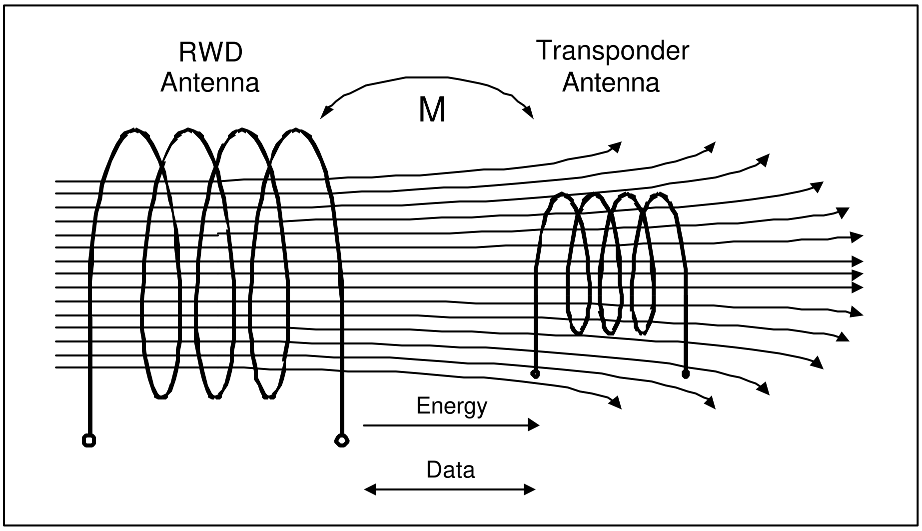
The following block diagram shows in principle the HITAG system configuration.



A control and data processing unit controls the modulation of the carrier signal and processes data coming back from the demodulator circuit.

7.2 Energy Transmission

Passive transponders must somehow be supplied with energy to be able to operate. In the HITAG System, this is achieved by using the principle of a loose coupled transformer:

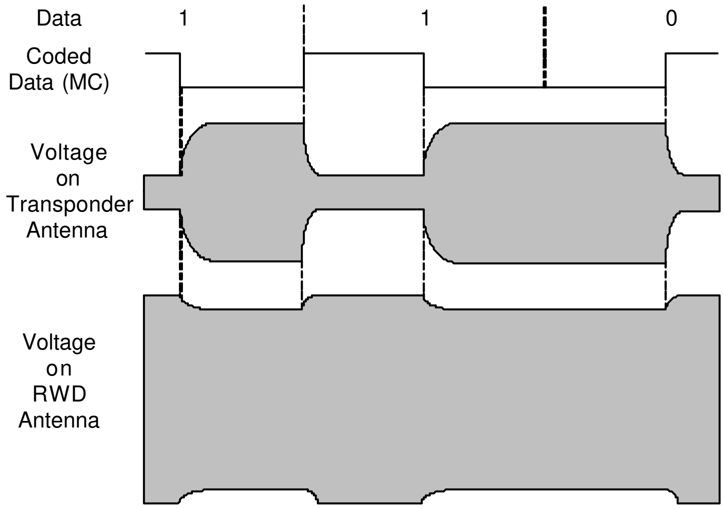


The RWD antenna generates a magnetic field. Some of the generated magnetic flux flows through the transponder antenna and induces a voltage there. The voltage drives a current and the transponder will start operating. As this current will be very small when the transponder is far away from the antenna, the HITAG S Transponder IC is designed for low power consumption.

The principle of a loose coupled transformer enables also a bi-directional data transmission.

7.3 Data Transmission: Transponder → Read/Write Device

For data transmission from the HITAG S Transponder to the RWD, the implemented method is called 'load modulation'. Here the HITAG S Transponder continuously changes the load on the magnetic field, by in principle turn on/off a resistor, according to the information to transmit. Alteration of the magnetic field is detected by the receiver of the RWD.

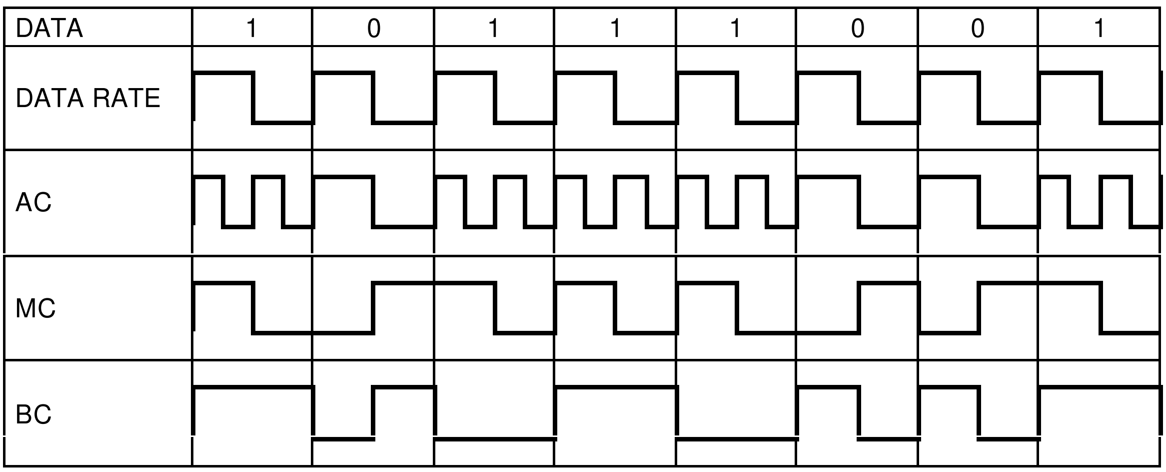


The modulation ratio of the RWD antenna voltage depends on the coupling factor of the antenna configuration (RWD antenna size, transponder antenna size, distance between the antennas,...).

7.3.1 CODING

Three different coding techniques for different States and Modes of the HITAG S Transponder IC are used (see also chapters “Command Set" and “Transponder Talks First (TTF) Mode”):

- AC: **A**ntiCollision **C**oding in Init State
- MC: **M**anchester **C**oding in Selected State and in Transponder Talks First State
- BC: **B**iphase **C**oding in Transponder Talks First State



A high level of the above coding signals means the physical state ‘modulator on’ (field loaded), a low level means ‘modulator off’ (field unloaded).

7.3.2 DATA RATE

The data rate for HITAG S Transponder in Reader Talks First (RTF) Mode depends on the corresponding UID REQUEST xx command.

For Tag Talks First (TTF) Mode the data rate can be defined by configuration.

Mode	Coding	Bit Rate	Bit Length
HITAG S RTF Mode	AC	2 kBit/s	64 T_0
		4 kBit/s	32 T_0
	MC	4 kBit/s	32 T_0
		8 kBit/s	16 T_0
HITAG S TTF Mode	MC	2 kBit/s	64 T_0
		4 kBit/s	32 T_0
		8 kBit/s	16 T_0
	Biphase	2 kBit/s	64 T_0
		4 kBit/s	32 T_0
		8 kBit/s	16 T_0

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

7.4 Data Transmission: Read/Write Device → Transponder

Data are transmitted to the transponder using Amplitude Shift Keying (ASK) modulation with a modulation index of 100 %. When the field is switched off, the physical state is named low field, otherwise high field.

7.4.1 CODING

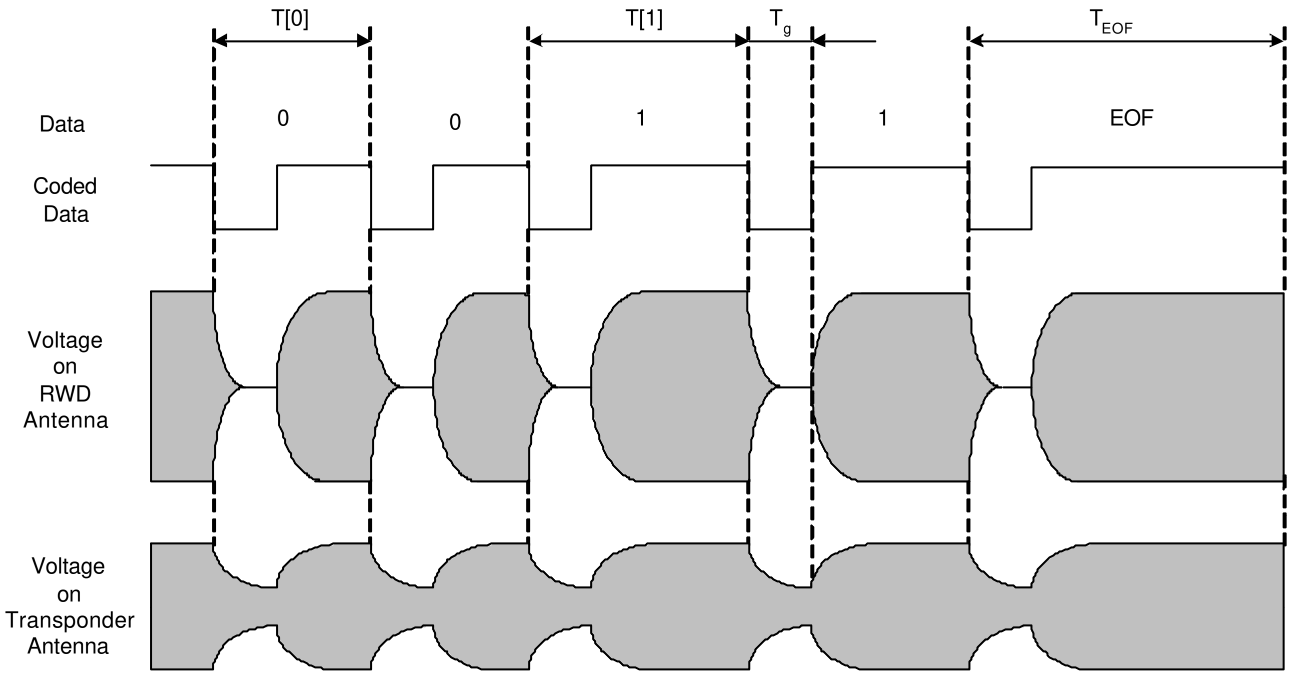
Binary Pulse Length Coding (BPLC) is used to encode the data stream.

All coded data Bits and the end of frame (EOF) condition start with a low field of length T_g.

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 characterised by a end of frame condition.

The following figure shows the data transmission from the Read/Write Device to the transponder.



Symbol	Description	Duration
T_g	Gap time	4..10 T_0 *)
T[0]	Logic 0 Bit length	18..22 T_0*)
T[1]	Logic 1 Bit length	26..30 T_0*)
T_{EOF}	Duration for end of frame condition	> 36 T_0

*) This application specific values must be within this frame, but have to be optimised for each application depending on rise and decay times of the RWD antenna voltage and the transponder antenna quality factor!

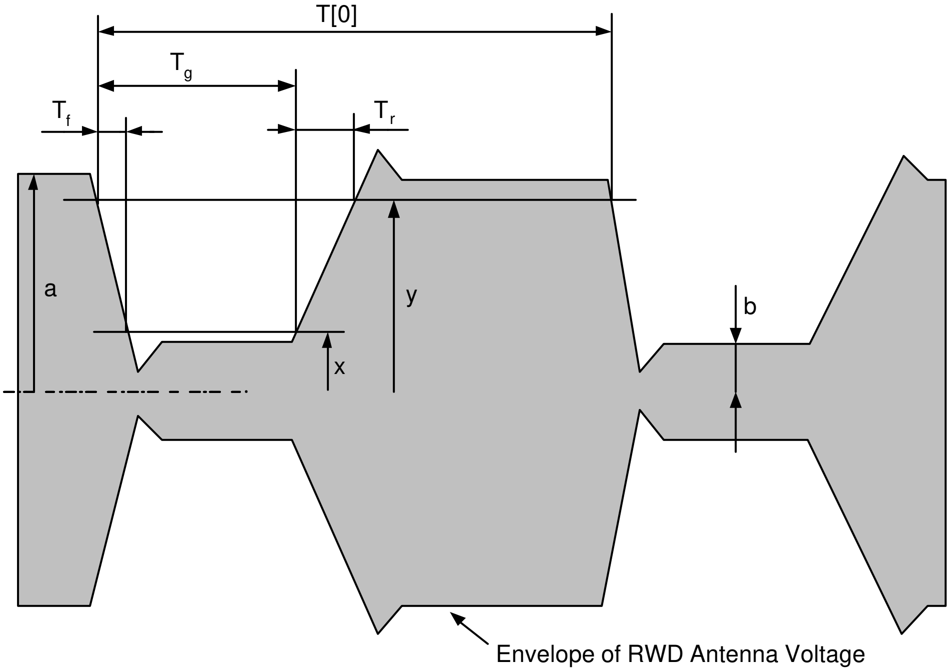
T_0 Carrier period time ($^1/_{125kHz}$ = 8 µs nominal)

The average Bit rate from the Read/Write Device to the HITAG S 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 the Read/Write Device to the HITAG S Transponder has to be a EOF condition.

7.4.2 MODULATION DETAILS



$x = 0.15\ a$, $y = 0.95\ a$

$m = (a - b) / (a + b)$.....Modulation index

Symbol	Min	Max
m	90 %	100 %
T_f	0	t.b.d.
T_r	0	t.b.d.

The following table shows two examples of modulation timing parameters for typical short- and long range applications.

Symbol	Short range application	Long range application
T_g	6 T_0	9 T_0
T[0]	20 T_0	22 T_0
T[1]	28 T_0	28 T_0
T_f	3 T_0	4 T_0
T_r	5 T_0	6 T_0

8 CONFIGURATION

8.1 Configuration Page

Memory Page 1 contains the three configuration Bytes CON 0, CON 1 and CON 2 (see 'Memory Organisation').

Changes on the Configuration Bytes are only active after a power on reset of the HITAG S Transponder.

CON0: Memory Type Information

CON 0

MSB							LSB
RES 5	RES 4	RES 3	RES 2	RES 1	RES 0	MEMT 1	MEMT 0

The following table describes the **Mem**ory **T**ype Bits MEMT 0 and MEMT 1 of configuration byte CON 0.

MEMT 1	MEMT 0	Memory Type
0	0	32 Bit
0	1	256 Bit
1	0	2048 Bit
1	1	Reserved

Bits RES 0 to RES 5 are reserved for future use.
Only Read access to configuration byte CON 0 is possible.

CON 1: Mode and Lock Bits

CON 1

MSB							LSB
AUT	TTFC	TTFDR 1	TTFDR 0	TTFM 1	TTFM 0	LCON	LKP

If the **Aut**hentication Bit AUT = '0' the HITAG S Transponder IC is configured in Plain Mode and can be Selected directly by the SELECT (UID) command and the corresponding UID. For Bit AUT = '1' the HITAG S Transponder IC is configured in Authentication Mode and can only be Selected with the SELECT (UID) command and a following secure CHALLENGE sequence (see also chapters 'State Diagram' and 'Command Set').

AUT	HITAG S Mode
0	Plain
1	Authentication

The **T**ransponder **T**alks **F**irst **C**oding Bit TTFC defines the used coding during transmitting data to the RWD. This effects the TTF State only.

TTFC	Coding in TTF State
0	Manchester
1	Biphase

The **T**ransponder **T**alks **F**irst **D**ata **R**ate Bits TTFDR 0 and TTFDR 1 define the used data rate during transmitting data to the RWD. This effects the TTF State only.

TTFDR 1	TTFDR 0	Data rate in TTF State
0	0	4 kBit
0	1	8 kBit
1	0	2 kBit
1	1	2 kBit and Pigeon Race Standard

The **T**ransponder **T**alks **F**irst **M**ode Bits TTFM 0 and TTFM 1 defines the number of Pages continuously transmitted to the RWD. This effects the TTF State only.

TTFM 1	TTFM 0	Pages transmitted in TTF State
0	0	TTF Mode disabled (= RTF Mode)
0	1	Page 4, Page 5
1	0	Page 4, Page 5, Page 6, Page 7
1	1	Page 4

The **L**ock **Con**figuration Bit LCON defines the access rights of the configuration Bytes CON 1 and CON 2. This Bit is one time programmable (OTP).

LCON	Access right CON 1 and CON 2
0	Read / Write
1	CON 1: Read Only CON 2: OTP

The **L**ock **K**ey and **P**assword Bit LKP defines the access rights of the PWDH 0 Byte of Page 1, password low Bytes and key high Bytes of Page 2 and key low Bytes of Page 3 when configured in Authentication Mode. In Plain Mode this Bit can be used to lock the user data of Page 2 and Page 3.

LKP	Access right key and password/Page 2 and Page 3
0	Read / Write
1	Read Only in Plain Mode No Access in Authentication Mode

Attention: In order to prevent further access to key and password, the following procedure must take place: After setting Bit LKP to ‘1’ the Lock Configuration Bit LCON must be set to ‘1’, because the Bit LKP has no OTP functionality!

CON 2: Memory Lock Bits

CON 2

MSB							LSB
LCK 7	LCK 6	LCK 5	LCK 4	LCK 3	LCK 2	LCK 1	LCK 0

Bit	Function	Access rights	Comment
LCK 7	Lock Page 4 and Page 5	0...Read / Write 1...Read Only	OTP if LCON = ‘1’ If Pigeon Race Standard is enabled (TTFDR 0 = TTFDR 1 = ‘1’) 16 Bits (Data 3 u. Data 2) of Page 5 remain still Read/Write accessible for LCK 7 = ‘1’
LCK 6	Lock Page 6 and Page 7	0...Read / Write 1...Read Only	OTP if LCON = ‘1’
LCK 5	Lock Page 8 – Page 11	0...Read / Write 1...Read Only	OTP if LCON = ‘1’
LCK 4	Lock Page 12 – Page 15	0...Read / Write 1...Read Only	OTP if LCON = ‘1’
LCK 3	Lock Page 16 – Page 23	0...Read / Write 1...Read Only	OTP if LCON = ‘1’
LCK 2	Lock Page 24 – Page 31	0...Read / Write 1...Read Only	OTP if LCON = ‘1’
LCK 1	Lock Page 32 – Page 47	0...Read / Write 1...Read Only	OTP if LCON = ‘1’
LCK 0	Lock Page 48 – Page 63	0...Read / Write 1...Read Only	OTP if LCON = ‘1’

8.2 Delivery Configuration

8.2.1 HITAG S32

This delivery configuration is valid for the following HITAG S 32 types:

HTS IC H32 01 DW/V4
HTS MO H32 01 DV
HTS FC H32 01 DV/VH

MSByte			LSByte
MSB LSB	MSB LSB	MSB LSB	MSB LSB
UID 3	UID 2	UID 1	UID 0

The 32 Bit Unique Identifier (UID) is programmed during the manufacturing process. Access rights: Read Only (RO)

On a Select (UID) command the HITAG S32 Transponder IC sends back three Reserved Bytes and the Byte CON 0 containing the Memory Type Information.

MSByte			LSByte
MSB LSB	MSB LSB	MSB LSB	MSB LSB
X	X	X	CON 0

CON 0							
MSB							LSB
X	X	X	X	X	X	0	0

The content of Bits and Bytes marked with 'X' are **not** defined at delivery!

8.2.2 HITAG S256

This delivery configuration is valid for the following HITAG S 256 types:

HTS IC H56 01 DW/V4
HTS MO H56 01 DV
HTS FC H56 01 DV/VH

	MSByte			LSByte
Page Address	MSB LSB	MSB LSB	MSB LSB	MSB LSB
0x00	UID 3	UID 2	UID 1	UID 0
0x01	0xAA	0x00	0x00	CON 0
0x02	0x4E	0x4F	0x54	0x48
0x03	0x52	0x4B	0x49	0x4D
0x04	X	X	X	X
0x05	X	X	X	X
0x06	X	X	X	X
0x07	X	X	X	X

CON 0

MSB							LSB
X	X	X	X	X	X	0	1

The content of Bits and Bytes marked with 'X' are **not** defined at delivery!

- The 32 Bit Unique Identifier (UID) is programmed during the manufacturing process.
- Modes: Reader Talks First (RTF), Plain
- Access Rights:
  UID: Read Only
  Page 1: Read/Write with exception of byte CON 0 (Read Only)
  Page 2 – Page 7: Read/Write

8.2.3 HITAG S2048

This delivery configuration is valid for the following HITAG S 2048 types:

HTS IC H48 01 DW/V4
HTS MO H48 01 DV
HTS FC H48 01 DV/VH

	MSByte			LSByte
Page Address	MSB LSB	MSB LSB	MSB LSB	MSB LSB
0x00	UID 3	UID 2	UID 1	UID 0
0x01	0xAA	0x00	0x00	CON 0
0x02	0x4E	0x4F	0x54	0x48
0x03	0x52	0x4B	0x49	0x4D
0x04	X	X	X	X
0x05	X	X	X	X
0x3E	X	X	X	X
0x3F	X	X	X	X

CON 0

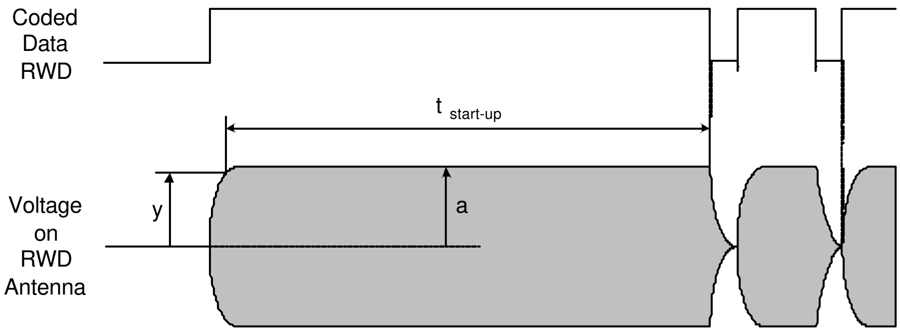
MSB							LSB
X	X	X	X	X	X	1	0

The content of Bits and Bytes marked with 'X' are **not** defined at delivery!

- The 32 Bit Unique Identifier (UID) is programmed during the manufacturing process.
- Modes: Reader Talks First (RTF), Plain
- Access Rights:
  UID: Read Only
  Page 1: Read/Write with exception of byte CON 0 (Read Only)
  Page 2 – Page 63: Read/Write

9 PROTOCOL TIMING

9.1 HITAG S Transponder Start up Time



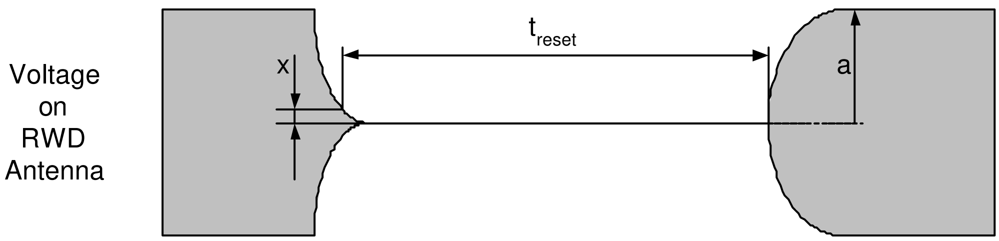
y = 0.95 a

After switching on the powering field, the Read/Write Device has to wait $t_{start-up}$ before sending the first command. After $t_{start-up}$ the HITAG S Transponder IC is in Ready State .

	MIN	TYP	MAX	Unit
$t_{start-up}$		245	t.b.d.	T_0

9.2 HITAG S Transponder Reset Time

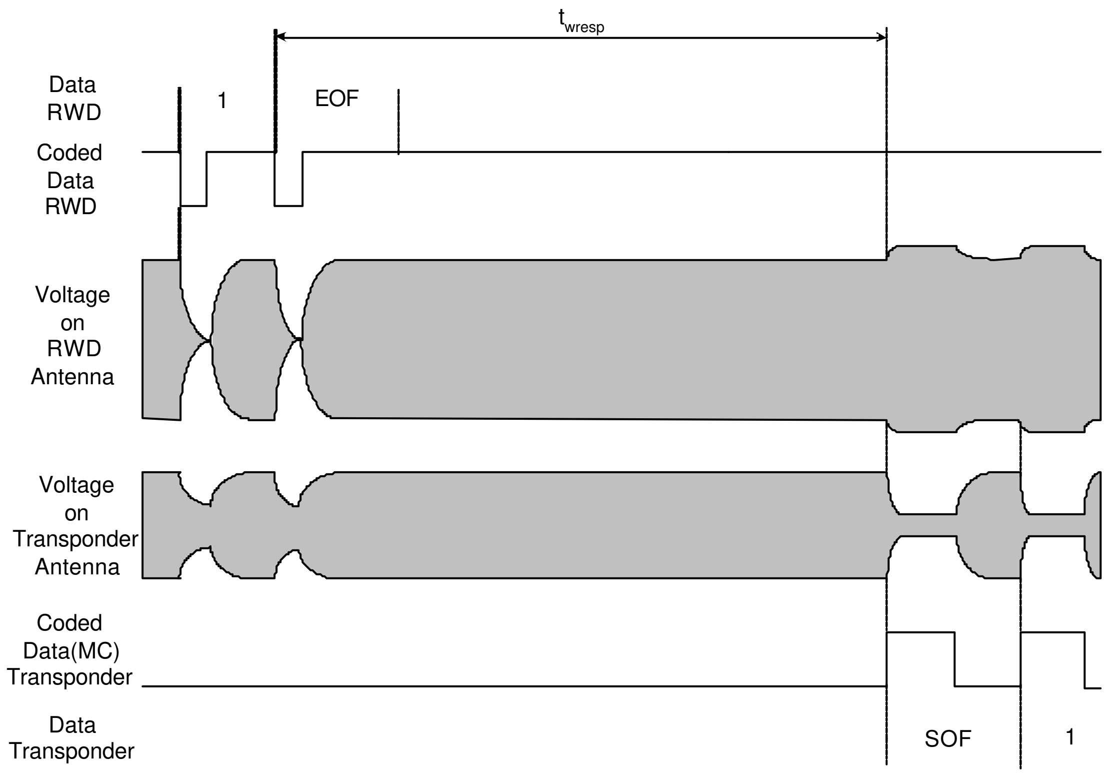
The powering field must be switched off for at least t_{reset} = 2 ms to generate a reset of the HITAG S IC and to enter it into Power Off State.



x = 0.15 a

	MIN	TYP	MAX	Unit
t_{reset}	2			ms

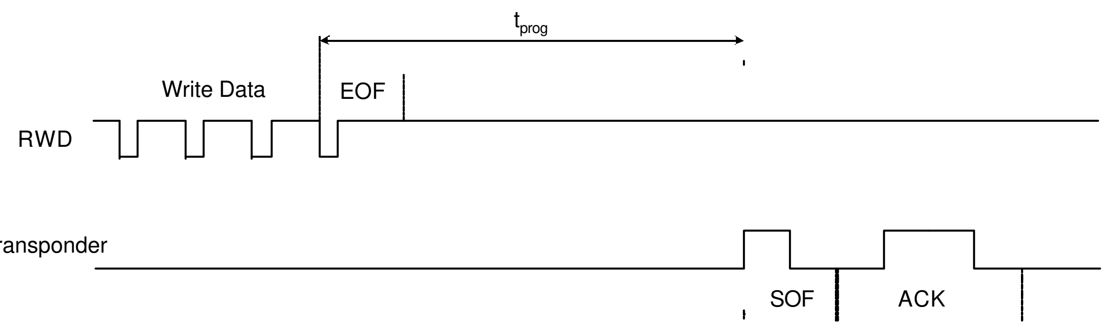
9.3 HITAG S Transponder waiting time before transmitting a response after receiving an EOF



When receiving a End of Frame (EOF) condition from the Read/Write Device, the transponder waits t_{wresp} before transmitting data.

	MIN	TYP	MAX	Unit
t_{wresp}	204	208	212	T_0

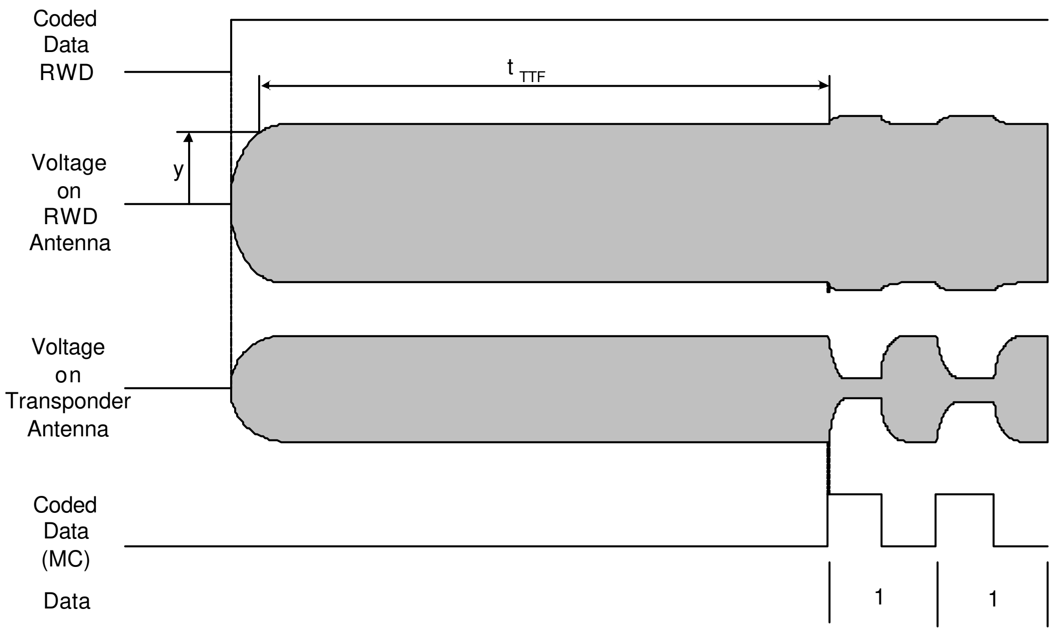
9.4 HITAG S Transponder programming time



When receiving the EOF of the write data from the Read/Write Device, the transponder waits t_{prog} before transmitting the SOF and acknowledge to confirm correct programming.

	MIN	TYP	MAX	Unit
t_{prog}	716	721	726	T_0

9.5 HITAG S Transponder waiting time before transmitting data in TTF Mode

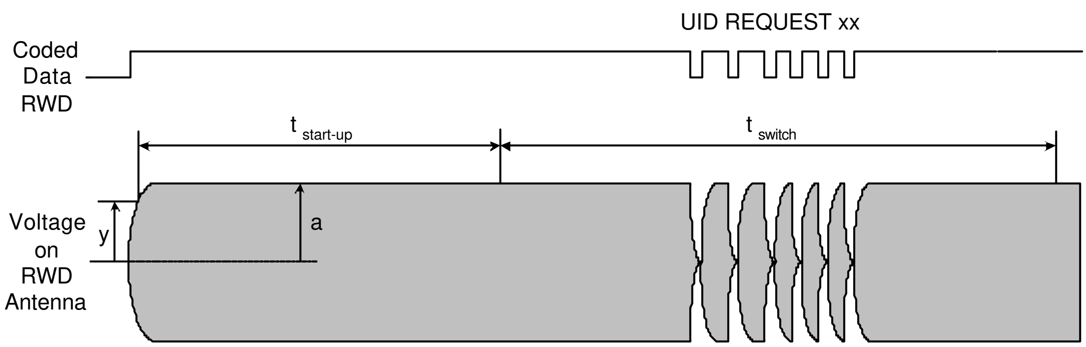


y = 0.95 a

After switching on the powering field, the HITAG S Transponder waits a time t_{TTF} before transmitting data if it is configured in TTF Mode.

	MIN	TYP	MAX	Unit
t_{TTF}	580	610	640	T_0

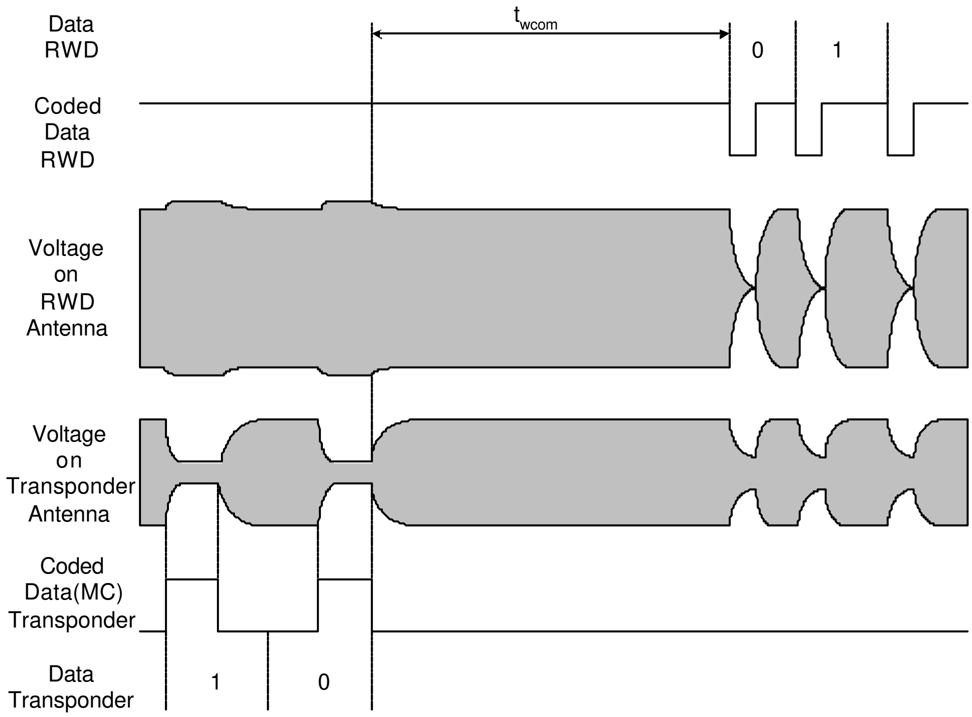
9.6 HITAG S Transponder Mode switching window



Within the time t_{switch} a HITAG S Transponder configured in TTF Mode can be switched into RTF Mode by a UID REQUEST xx command. The HITAG S Transponder responds to this command with the UID and changes into Init State .

	MIN	TYP	MAX	Unit
t_{switch}	t.b.d.	320	t.b.d	T_0

9.7 Read/Write Device waiting time before sending a subsequent command



When the Read/Write Device has received the response from the HITAG S Transponder to a previous command, the RWD has to wait a time t_{wcom} before sending a subsequent command or Write data after a Write command.

Data transmitted to the HITAG S Transponder within t_{wcom}, will not be recognised.

	MIN	TYP	MAX	Unit
t_{wcom}	90			T_0

10 STATE DIAGRAM

10.1 General description of State s

Power Off

The powering magnetic field is switched off or the HITAG S Transponder is out of field

Ready

After start up phase, the HITAG S Transponder is ready to receive the first command.

Init

The HITAG S Transponder enters this State after the first UID REQUEST xx command.
In this State the Response Protocol Mode (see chapter 'Command Set') may be changed by further UID REQUEST xx commands.
If there are several HITAG S Transponders in the field of the RWD antenna at the same time, the AC SEQUENCE can be started to determine the UID of every HITAG S Transponder.

Authenticate

The HITAG S Transponder enters this State after a valid SELECT (UID) command when configured in Authentication Mode.
After a encrypted CHALLENGE Authentication the HITAG S Transponder changes into the Selected State.

Selected

The HITAG S Transponder enters this State after a valid SELECT (UID) command when configured in Plain Mode or by a SELECT (UID) and CHALLENGE sequence when configured in Authentication Mode.
Only one HITAG S Transponder in the field of the RWD antenna can be Selected at the same time.
In this State, Read and Write operations from and to the memory are possible.

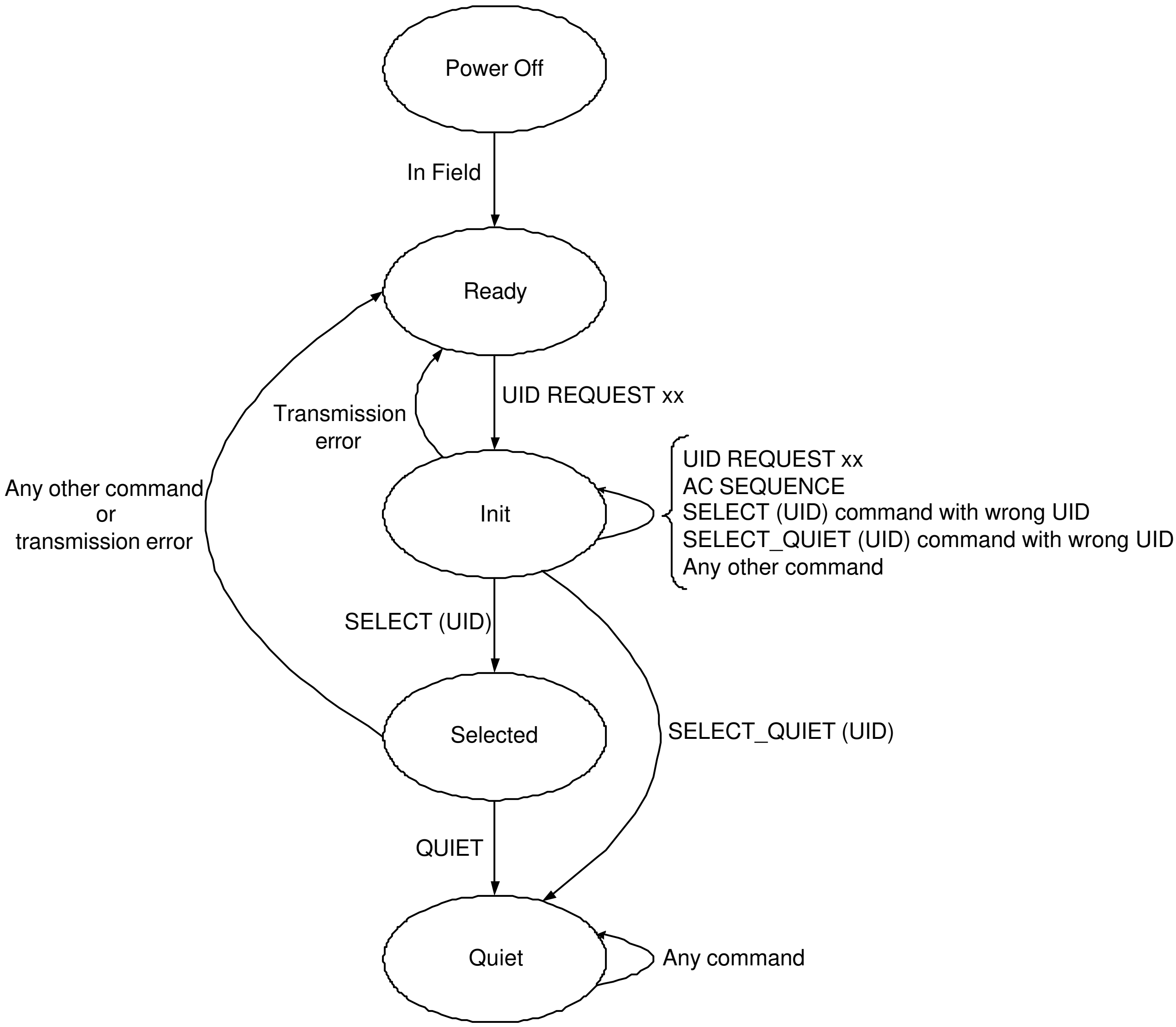
Quiet

The HITAG S Transponder enters this State after a SELECT_QUIET command in Init State or a QUIET command in Selected State.
In this State, the HITAG S Transponder will not answer to any command.
Switching off the powering magnetic field or moving the HITAG S Transponder out of field enters it into the Power Off State.

Transponder Talks First (TTF)

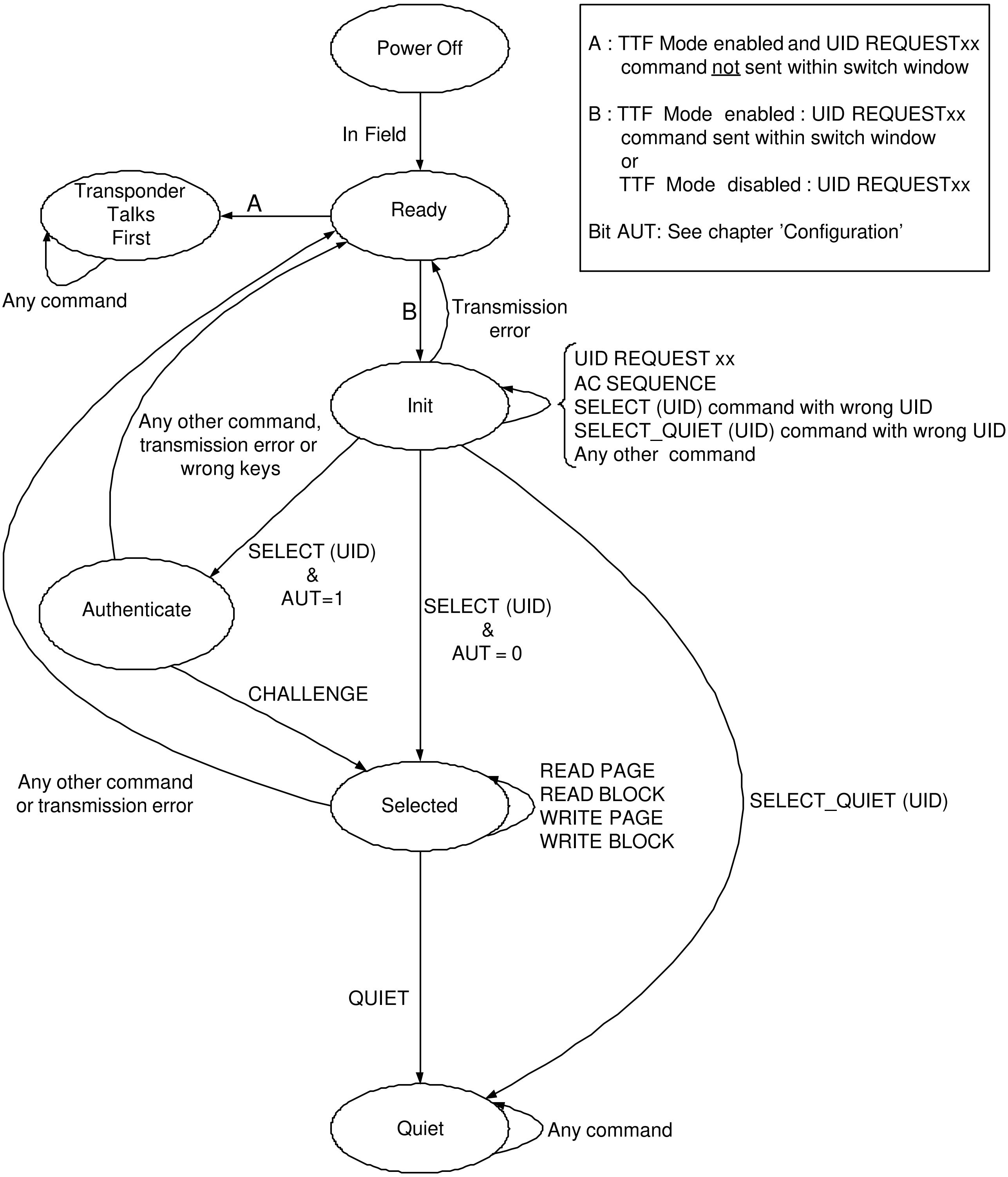
The HITAG S Transponder enters this State when configured in TTF Mode and without receiving a UID REQUEST xx command within the Mode switch window.
In this State, the HITAG S Transponder continuously transmits data with configurable data coding, data rate and data length.

10.2 HITAG S32



Note:
Switching off the powering magnetic field or moving the HITAG S Transponder out of the RWD antenna field, enters the HITAG S Transponder into the Power Off State, independently of its previous State.

10.3 HITAG S256 and HITAG S2048



Note:
Switching off the powering magnetic field or moving the HITAG S Transponder out of the RWD antenna field, enters the HITAG S Transponder into the Power Off State, independently of its previous State.

11 COMMAND SET

11.1 General Comments

For HITAG S 32 only the commands described in the corresponding State diagram are valid commands.

11.2 UID REQUEST xx

	MSB LSB	
RWD:	UID REQUEST xx	EOF

			LSByte			MSByte
			MSB LSB	MSB LSB	MSB LSB	MSB LSB
Transponder:	t_{wresp}	SOF	UID 0	UID 1	UID 2	UID 3
		N =	1............8	9....**k**...16	17.......24	25.......32

N...Bit position
k...Any collision position (see command AC SEQUENCE)

After the RWD transmits this command, all HITAG S Transponders located in the field of the RWD antenna respond with a start of frame pattern followed by the corresponding 32 Bit UID. The complete response of the HITAG S Transponder is transmitted in Anticollision Coding (AC, see section 7.3.1 Coding).

Coding:	MSB LSB	Response Protocol Mode
UID REQUEST Std	0 0 1 1 0	Standard
UID REQUEST Adv	1 1 0 0 x	Advanced
UID REQUEST FAdv	1 1 0 1 0	Fast Advanced

x... can be ‘0’ or ‘1’

The Response Protocol Mode defined by the corresponding UID Request command determines the coding, data rate and the SOF pattern of the HITAG S Transponder response.

Response Protocol Mode	SOF	Coding	Data Rate
Standard	‘1’	AC	2 kBit/s
Advanced	‘111’	AC	2 kBit/s
Fast Advanced	‘111’	AC	4 kBit/s

A HITAG S Transponder in Ready State changes into Init State after receiving a correct UID REQUEST xx command.

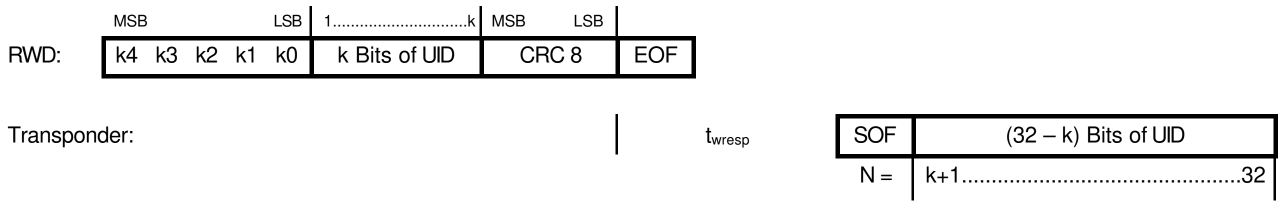
A HITAG S Transponder being already in Init State remains in Init State after receiving a further correct UID REQUEST xx command.

Always the latest UID REQUEST xx command defines the Response Protocol Mode for the following commands.

11.3 AC SEQUENCE

If more than one HITAG S Transponder is in the field of the antenna a special designed RWD recognises the first collision at the **Bit position N = k** of the UID response. As a result the RWD starts an **A**nti**c**ollision Sequence (AC SEQUENCE).

This command consists of a 5 Bit number (k4 to k0) with the Bit position k where the collision occurred followed by (k - 1) Bits of the recognised UID and a Bit (one or zero) at the collision position. An 8 Bit CRC (cyclic redundancy check) of this sequence is also sent to the transponders.



After transmitting this command, all HITAG S Transponders which first k Bits of the own UID match with the k received UID Bits, answer with the SOF and the rest of their own UID.

If a collision occurs again the described cycle has to be repeated until one UID is determined.

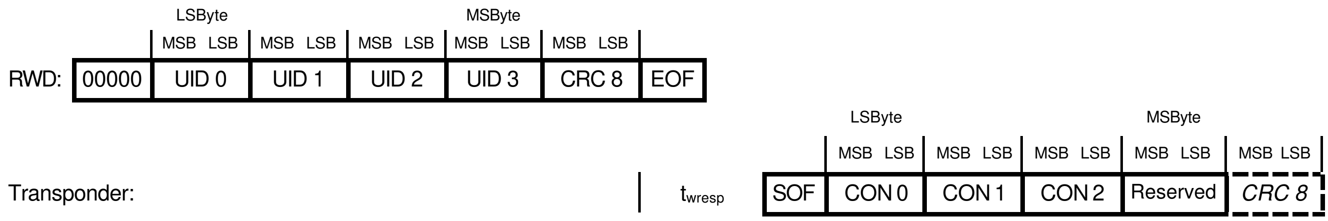
The complete response of the HITAG S Transponder is transmitted in Anticollision Coding (AC).

Response Protocol Mode	SOF	Coding	Data Rate
Standard	‘1’	AC	2 kBit/s
Advanced	‘111’	AC	2 kBit/s
Fast Advanced	‘111’	AC	4 kBit/s

During the AC SEQUENCE commands the HITAG S Transponder stays in Init State . **Even those HITAG S Transponders where the k received Bits of the UID do not match remain in Init State.**

11.4 SELECT (UID)

The SELECT (UID) command consists of 5 Zero-Bits followed by the determined 32 Bit UID and an 8 Bit Cyclic Redundancy Check (CRC). The selected transponder then responds with a start of frame pattern (SOF) followed by the content of the Configuration Page and dependent on the Response Protocol Mode with an 8 Bit CRC.



The complete response of the HITAG S Transponder is transmitted in Manchester Coding (MC).

In Plain Mode the MSByte of Page 1 is a Reserved Byte, in Authentication Mode this Byte contains the password high Byte PWDH 0. At the response on a SELECT (UID) command of a HITAG S Transponder configured in Authentication Mode (Bit AUT = 1, keys and password locked), this PWDH 0 Byte is dissolved by 8 One Bits.

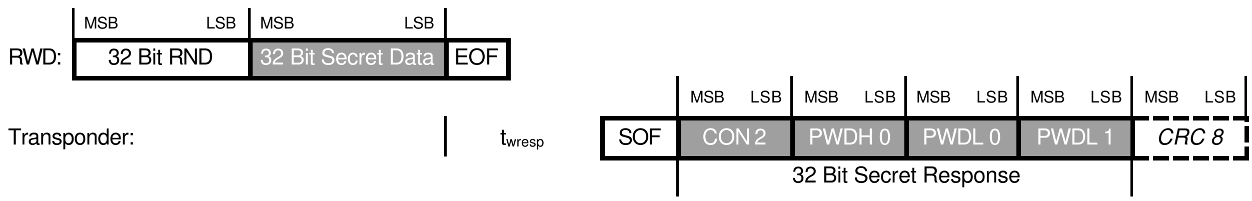
Response Protocol Mode	SOF	CRC 8	Coding	Data Rate
Standard	‘1’	no	MC	4 kBit/s
Advanced	‘111111’	yes	MC	4 kBit/s
Fast Advanced	‘111111’	yes	MC	8 kBit/s

In Plain Mode (Bit AUT = 0) the HITAG S Transponder changes into Selected State after receiving a correct SELECT (UID) command

In Authentication Mode (Bit AUT = 1) the HITAG S Transponder changes into Authenticate State after receiving a correct SELECT (UID) command and waits for the CHALLENGE command.

11.5 CHALLENGE

By means of the response of the SELECT (UID) command the RWD recognises that the HITAG S Transponder is configured in Authentication Mode (Bit AUT = 1) and starts the encrypted Challenge sequence.



The Read/Write Device sends a 32 Bit Random Number (RND) and a 32 Bit secret data stream to the transponder. In order to perform the secret data stream, the Philips security coprocessor HT RC130 is required. If the received secret data stream corresponds with the secret data stream calculated by the HITAG S Transponder, a 32 Bit Secret Response (secret data stream encrypting the configuration byte CON 2, password high byte PWDH 0 and password low Bytes PWDL 0 and PWDL 1) is transmitted after the SOF.

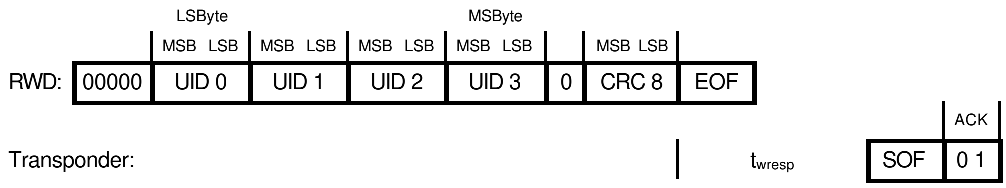
The response of the HITAG S Transponder is transmitted in Manchester Coding (MC).

Response Protocol Mode	SOF	CRC 8	Coding	Data Rate
Standard	‘1’	no	MC	4 kBit/s
Advanced	‘111111’	yes	MC	4 kBit/s
Fast Advanced	‘111111’	yes	MC	8 kBit/s

A HITAG S Transponder configured in Authentication Mode changes from Authenticate State into Selected State only after a correct CHALLENGE Sequence.

11.6 SELECT_QUIET (UID)

With this command a HITAG S Transponder in Init State can be directly entered into the Quiet State.



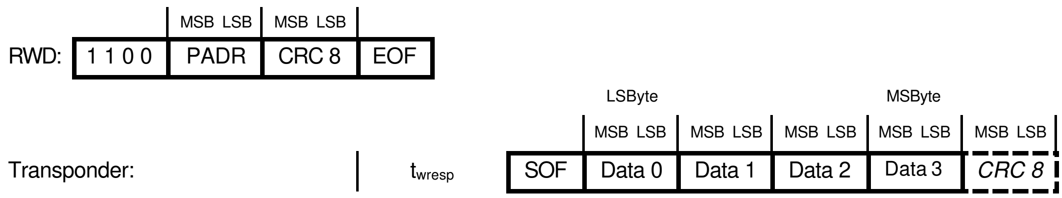
The ‘start of frame’ (SOF) pattern and the acknowledge (ACK) is transmitted in Manchester Coding.

Response Protocol Mode	SOF	Coding	Data Rate
Standard	‘1’	MC	4 kBit/s
Advanced	‘111111’	MC	4 kBit/s
Fast Advanced	‘111111’	MC	8 kBit/s

A HITAG S Transponder, once entered the Quiet State can only be enabled by switching off the powering magnetic field for at least a time t_{reset} or the HITAG S Transponder must be moved out of the antenna field (Power Off State).

11.7 READ PAGE

After a HITAG S Transponder was selected by the corresponding SELECT (UID) command (or SELECT (UID) and CHALLENGE for Authentication Mode) a read operation of data stored on the EEPROM can be performed. After transmitting the READ PAGE command, the Page address PADR (8 Bits) and the 8 Bit Cyclic Redundancy Check CRC 8, the HITAG S Transponder responds with the SOF and 32 Bits data of the corresponding Page.

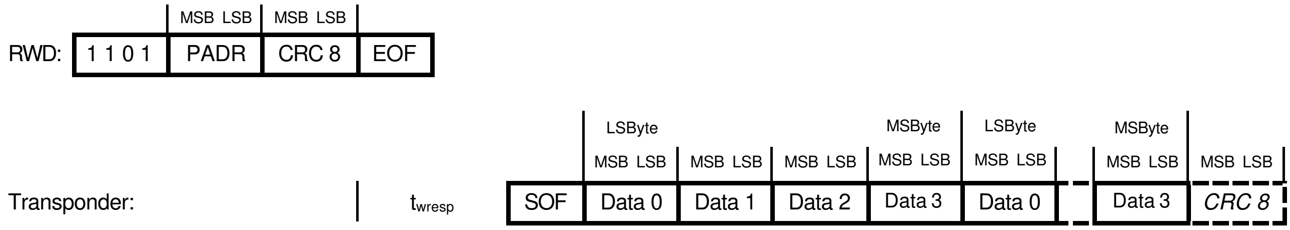


The highest Page address (PADR) is 0x 3F, therefore the two highest Bits must be ‘0’.

Response Protocol Mode	SOF	CRC 8	Coding	Data Rate
Standard	‘1’	no	MC	4 kBit/s
Advanced	‘111111’	yes	MC	4 kBit/s
Fast Advanced	‘111111’	yes	MC	8 kBit/s

11.8 READ BLOCK

After transmitting the READ BLOCK command, the Page address PADR within a block and the 8 Bit Cyclic Redundancy Check CRC 8, the HITAG S Transponder responds with the SOF and 32 up to 128 Bits of data beginning with the addressed Page within a Block to the last Page of the corresponding Block.

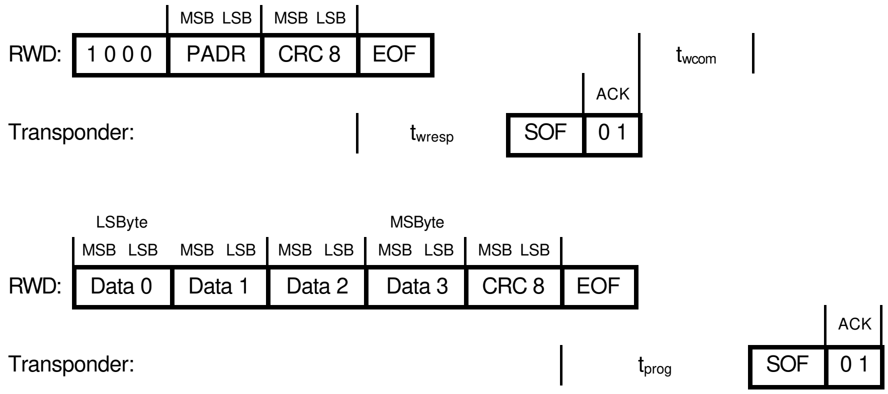


Response Protocol Mode	SOF	CRC 8	Coding	Data Rate
Standard	‘1’	no	MC	4 kBit/s
Advanced	‘111111’	yes	MC	4 kBit/s
Fast Advanced	‘111111’	yes	MC	8 kBit/s

11.9 WRITE PAGE

After a HITAG S Transponder was selected by the corresponding SELECT (UID) command (or SELECT (UID) and CHALLENGE for Authentication Mode) a write operation of data onto the memory can be carried out.

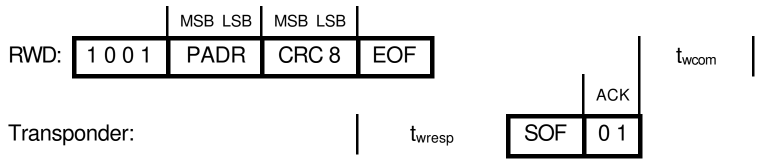
After transmitting the WRITE PAGE command, the Page address PADR and the 8 Bit Cyclic Redundancy Check (CRC 8), the HITAG S Transponder responds with the SOF and an acknowledge (ACK) to confirm the reception of a correct WRITE PAGE command. After the waiting time t_{wcom} the RWD transmits the write data with CRC 8 check. After the programming time t_{prog} the HITAG S Transponder responds with a SOF and an acknowledge to confirm correct programming.



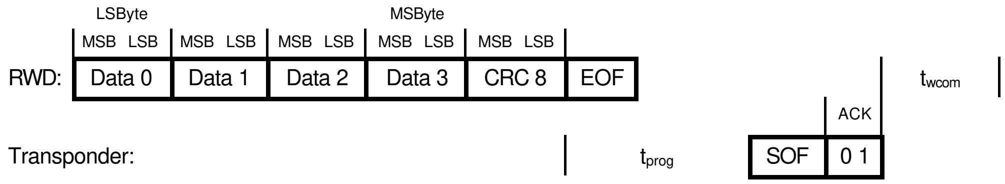
Response Protocol Mode	SOF	Coding	Data Rate
Standard	‘1’	MC	4 kBit/s
Advanced	‘111111’	MC	4 kBit/s
Fast Advanced	‘111111’	MC	8 kBit/s

11.10 WRITE BLOCK

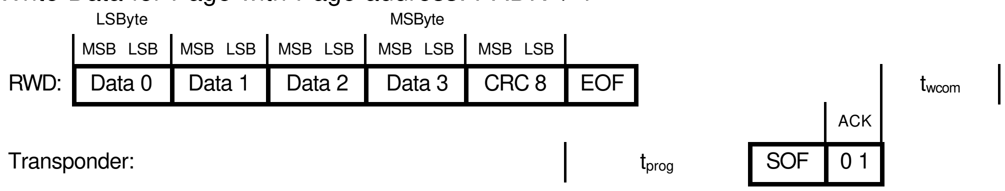
After transmitting the WRITE BLOCK command, the Page address PADR within a Block and the 8 Bit Cyclic Redundancy Check (CRC 8), the HITAG S Transponder responds with the SOF and an acknowledge (ACK) to confirm the reception of a correct WRITE BLOCK command. After the waiting time t_{wcom} the RWD transmits the write data with CRC 8 check Page by Page (1 to 4 Pages depending on the Page address PADR within the corresponding block). After the programming time t_{prog} the HITAG S Transponder responds with a SOF and an acknowledge to confirm correct programming of every Page.



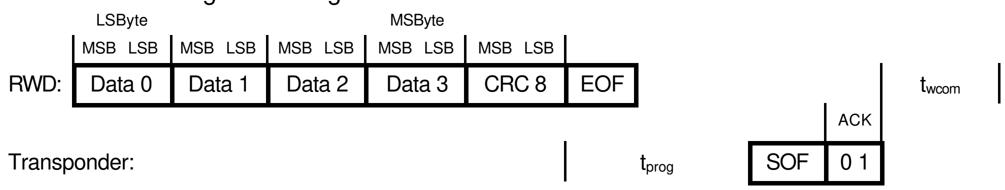
Write Data for Page with Page address: PADR



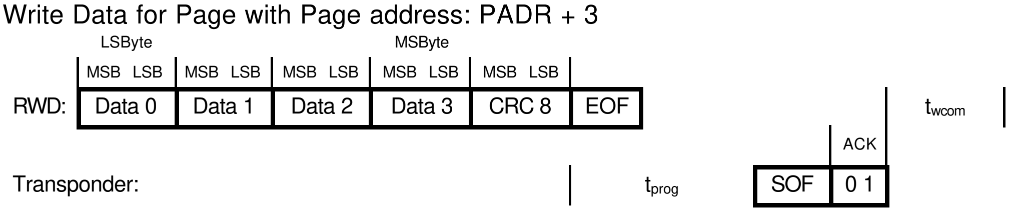
Write Data for Page with Page address: PADR + 1



Write Data for Page with Page address: PADR + 2



Write Data for Page with Page address: PADR + 3

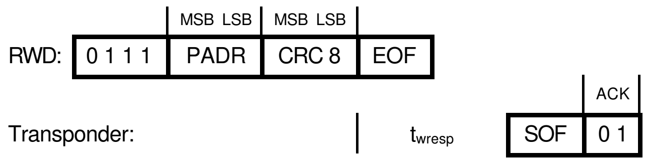


Response Protocol Mode	SOF	Coding	Data Rate
Standard	‘1’	MC	4 kBit/s
Advanced	‘111111’	MC	4 kBit/s
Fast Advanced	‘111111’	MC	8 kBit/s

11.11 QUIET

With this command a Selected HITAG S Transponder can be entered into the Quiet State.

A valid Page address (PADR) and Cyclic Redundancy Check (CRC 8) must be sent for command structure reasons only.



After the response wait time t_{wresp} the HITAG S Transponder responds with a SOF and an acknowledge to confirm entering the Quiet State.

Response Protocol Mode	SOF	Coding	Data Rate
Standard	‘1’	MC	4 kBit/s
Advanced	‘111111’	MC	4 kBit/s
Fast Advanced	‘111111’	MC	8 kBit/s

A HITAG S Transponder, once entered the Quiet State can only be enabled by switching off the powering magnetic field for at least a time t_{reset} or the HITAG S Transponder must be moved out of the antenna field (Power Off State).

12 TRANSPONDER TALKS FIRST (TTF) MODE

This special mode of the HITAG S Transponder enables data transmission to a Read/Write Device without sending any command. The TTF Mode can be enabled/disabled and configured by setting the corresponding Bits of the Configuration byte CON 1 (see chapter 'Configuration').

A HITAG S Transponder configured in TTF Mode can be switched temporarily into Reader Talks First (RTF) Mode by sending a UID REQUEST xx command within a defined window after turning on the powering field. The HITAG S Transponder will leave this temporarily RTF Mode after switching off the powering field or moving it out of the RWD antenna field.

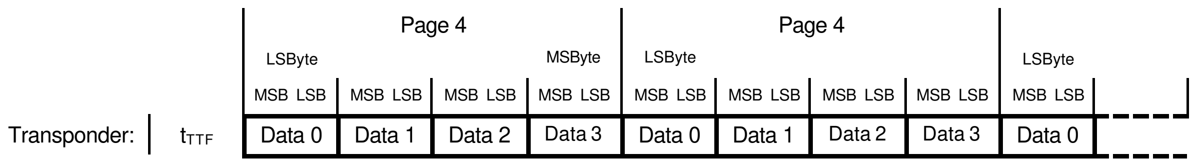
If the HITAG S Transponder is configured in TTF Mode and no Mode switch command is sent by the RWD within the defined switch window it enters the TTF State. Depending on the configuration, the HITAG S Transponder transmits the data with different coding, data rate and data length.
It is recommended to use some of the data bits as a well defined start sequence.

12.1 32 Bit TTF Mode

Configuration:

TTFM 1	TTFM 0
1	1

In this Mode, the HITAG S Transponder continuously transmits the data content of Page 4.



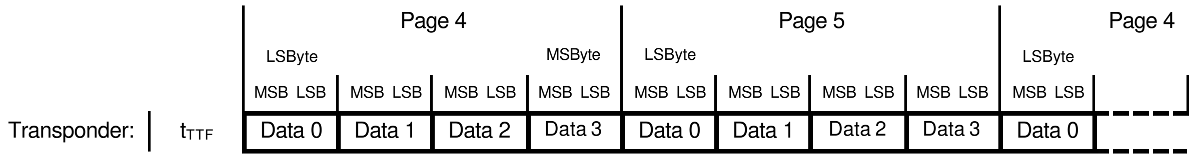
The data rate and the data coding can be chosen independently by configuration Bits TTFC, TTFDR 0 and TTFDR 1.

12.2 64 Bit TTF Mode

Configuration:

TTFM 1	TTFM 0
0	1

In this Mode, the HITAG S Transponder continuously transmits the data content of Page 4 and Page 5.



The data rate and the data coding can be chosen independently by configuration Bits TTFC, TTFDR 0 and TTFDR 1.

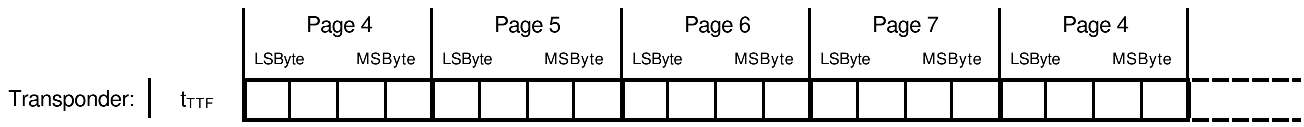
Note: This Mode may be used for Pigeon race standards.

12.3 128 Bit TTF Mode

Configuration:

TTFM 1	TTFM 0
1	0

In this Mode, the HITAG S Transponder continuously transmits the data content of Page 4, Page 5, Page 6 and Page 7.



The data rate and the data coding can be chosen independently by configuration Bits TTFC, TTFDR 0 and TTFDR 1.

Note: This Mode may be used for ISO 11784/85 Animal ID standard and German Waste Management standard (BDE) respectively.

13 DATA INTEGRITY / CALCULATION OF CRC

The following explanations show the features of the HITAG S protocol to protect read and write access to transponders from undetected errors.

13.1 Data Transmission: Read/Write Device to HITAG S Transponder

Every data stream transmitted by the Read/Write Device to the HITAG S Transponder includes an 8Bit Cyclic Redundancy Check (CRC 8). The data stream is first checked for data errors by the HITAG S Transponder and then executed.

The generator polynomial for the CRC 8 is:

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

The CRC pre set value is: 0xFF

13.2 Data Transmission: HITAG S Transponder to Read/Write Device

13.2.1 STANDARD RESPONSE PROTOCOL MODE

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

13.2.2 ADVANCED/FAST ADVANCED RESPONSE PROTOCOL MODE

In Advanced – and Fast Advanced Response Protocol Mode the response on a SELECT (UID) , CHALLENGE, READ PAGE, READ BLOCK command, includes a CRC 8 check sum.

The generator polynomial for the CRC 8 is:

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

The CRC pre set value is: 0xFF

13.3 Source Code for CRC-Checksum

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

```
#include <stdio.h>

#define CRC_PRESET  0xFF
#define CRC_POLYNOM 0x1D

void calc_crc(unsigned char * crc,
unsigned char data,
unsigned char Bitcount)
{
*crc ^= data;                   // crc = crc (exor) data
do
{
  if( *crc & 0x80 )             // if (MSB-CRC == 1)
  {
    *crc<<=1;                   // CRC = CRC Bit-shift left
    *crc ^= CRC_POLYNOM;        // CRC = CRC (exor) CRC_POLYNOM
  }
  else
  {
    *crc<<=1;                   // CRC = CRC Bit-shift left
  }

  printf("CRC: %02X ", *crc);   // output result step by step
} while(--Bitcount);
  printf("\n");
}


void main(void)
{
const cmd=0x00;    /* 5 Bit command, aligned to MSB */
const ident[4]={0x2C, 0x68, 0x0D, 0xB4 };


unsigned char crc;
int i;


crc = CRC_PRESET;  /* initialize crc algorithm */

calc_crc(&crc, cmd, 5); /* compute 5 crc Bits only */

for(i=0; i<4; i++)
calc_crc(&crc, ident[i], 8);

/* crc = 0x9E at this point */
printf("%02X\n",crc);

getch();

}
```

14 ABBREVIATIONS

AC	Anticollision Code
ASK	Amplitude Shift Keying
BC	Biphase Code
BPLC	Binary Pulse Length Coding
CRC	Cyclic Redundancy Check
EEPROM	Electrically Erasable Programmable Memory
EOF	End of frame
LSB	Least Significant Bit
LSByte	Least Significant Byte
m	Modulation Index
MC	Manchester Code
MSB	Most Significant Bit
MSByte	Most Significant Byte
NA	No Access
OTP	One Time Programmable.
RND	Random Number
RO	Read Only
RTF	Reader Talks First
R/W	Read/Write
RWD	Read/Write Device
SOF	Start of Frame
TTF	Transponder Talks First
UID	Unique Identifier

15 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.	

16 DISCLAIMERS

16.1 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 customers using or selling these products for use in such applications do so on their own risk and agree to fully indemnify Philips for any damages resulting from such improper use or sale.

17 REVISION HISTORY

REVISION	DATE	CPCN	PAGE	DESCRIPTION
1.0	August 2002			Initial version
1.1	October 2002		Complete Document Pages 29 – 33	Public Mode changed into Plain Mode Data Rate corrected for Manchester Coding Delivery Configuration added

NOTES

Philips Semiconductors - a worldwide company

Contact Information

For additional information please visit **http://www.semiconductors.philips.com**.Fax: **+31 40 27 24825**
For sales offices addresses send e-mail to: **sales.addresses@www.semiconductors.philips.com**.

SCA74