

DATA SHEET

PCF7936AS

Security Transponder (HITAG2)

Product Specification

2010 May 04

CONFIDENTIAL



Security Transponder (HITAG2)

PCF7936AS

CONTENT

1	FEATURES	4
2	GENERAL DESCRIPTION	4
3	ORDERING INFORMATION	4
4	BLOCK DIAGRAM	5
5	TYPICAL APPLICATION	5
6	QUICK REFERENCE DATA	6
7	FUNCTIONAL DESCRIPTION SECURITY TRANSPONDER	7
7.1	Memory Organization, EEPROM	7
7.1.1	Identifier, IDE	8
7.1.2	Password Basestation, PSW _B	8
7.1.3	Secret Key, SK	9
7.1.4	Transponder and Memory Configuration, TMCF	9
	Secret Key Lock, SKL	9
	Page 3 Lock, PG3L	9
	Protect Write User Page 4 and 5, PWP1	9
	Protect Write User Page 6 and 7, PWP0	9
	Enable Cipher Mode, ENC	9
	Mode Select, MS	10
	Data Coding Select, DCS	10
7.1.5	Password Transponder, PSW _T	10
7.1.6	User Pages, USER 0 to 3	10
7.2	Transponder State Diagram	11
7.2.1	WAIT State	11
7.2.2	AUTHORIZED State	12
7.2.3	HALT State	12
7.2.4	READ ONLY State	12
7.3	Command Set	13
7.3.1	Command Description	14
	HALT	15
	READ_PAGE	15
	READ_PAGE_INV	16
	START_AUTH (Password Mode)	17
	START_AUTH (Cipher Mode)	18
	WRITE_PAGE	19
7.4	Calculation Unit	20
7.5	Read Only Modes	21
7.5.1	ISO 11784/5 (MS1 = 0, MS0 = 0)	21
7.5.2	MIRO Mode (MS1 = 0, MS0 = 1)	21
7.5.3	PCF7931/30/35 (MS1 = 1, MS0 = 0)	21
7.6	Transponder Data Transmission Format	22
7.6.1	Read Direction	22
7.6.2	Write Direction	23
7.7	LF Field Power On Reset	24
8	EEPROM CONTENT AT DELIVERY	25
9	LIMITING VALUES	26
10	DEVICE CHARACTERISTICS	27
10.1	Electrical Characteristics	27
10.2	Timing Characteristics	28
10.3	Mechanical Characteristics	29
11	TEST SETUP	30
12	DEVELOPMENT TOOLS	31

Security Transponder (HITAG2)

PCF7936AS

13 REVISION HISTORY	31
14 LEGAL INFORMATION	32
14.1 Data sheet status	32
14.2 Definitions	32
14.3 Disclaimers	32

Security Transponder (HITAG2)

PCF7936AS

1 FEATURES

- Security Transponder for use in contactless authentication applications
- Data transmission and energy supply via LF link
- 32 bit quasi unique device identification (serial number) and product type identification.
- Fast mutual authentication, 39ms
- 48 bit Secret Key
- 256 bit EEPROM for user data storage (128 bit) and device configuration/personalization (128 bit)
- EEPROM read/write protection features
- 20 years non-volatile data retention
- More than 100 000 EEPROM erase/write cycles
- Once the memory has been erased by UV, access is denied
- Read Only emulation modes (H400x, ISO 11784/85 and PCF7931)
- Excellent sensitivity in read and write mode
- Automotive temperature range: -40°C to +85°C
- Leadless plastic stick package

2 GENERAL DESCRIPTION

The PCF7936AS is a high performance automotive proof Security Transponder for vehicle Immobilization applications, where the transponder has to identify itself towards the basestation as an authorized device.

The Security Transponder derives its power supply from the magnetic field (LF field) established by the basestation. No additional battery supply is needed. Data is transmitted by modulating the LF field.

The Security Transponder features secure contactless authentication, employing a Secret Key and a random number in order to cipher any communication between the device and the basestation. The secure contactless authentication is ideally suited for vehicle immobilization applications. In addition, the device features a factory programmed quasi unique serial number that also serves as product type identification.

If desired, the device may be operated as a Read/write transponder with access control by password or as a Read Only transponder.

3 ORDERING INFORMATION

EXTENDED TYPE NUMBER	PACKAGE			TEMPERATURE RANGE (°C)
	NAME	DESCRIPTION	OUTLINE VERSION	
PCF 7936AS/3851	SOT3851	leadless plastic stick package	SOT385-1	-40°C to +85°C
PCF 7936AS/3851/C	SOT3851	leadless plastic stick package	SOT385-1	-40°C to +85°C

Security Transponder (HITAG2)

PCF7936AS

4 BLOCK DIAGRAM

The PCF7936AS features a high degree of integration and incorporates the transponder chip, coil and capacitor assembled in a leadless stick package, see Figure 1.

Security Transponder

- Contactless Interface
- EEPROM (256 bit)
- Control Logic
- Calculation Unit (security algorithm)
- Reset Logic
- Test Logic

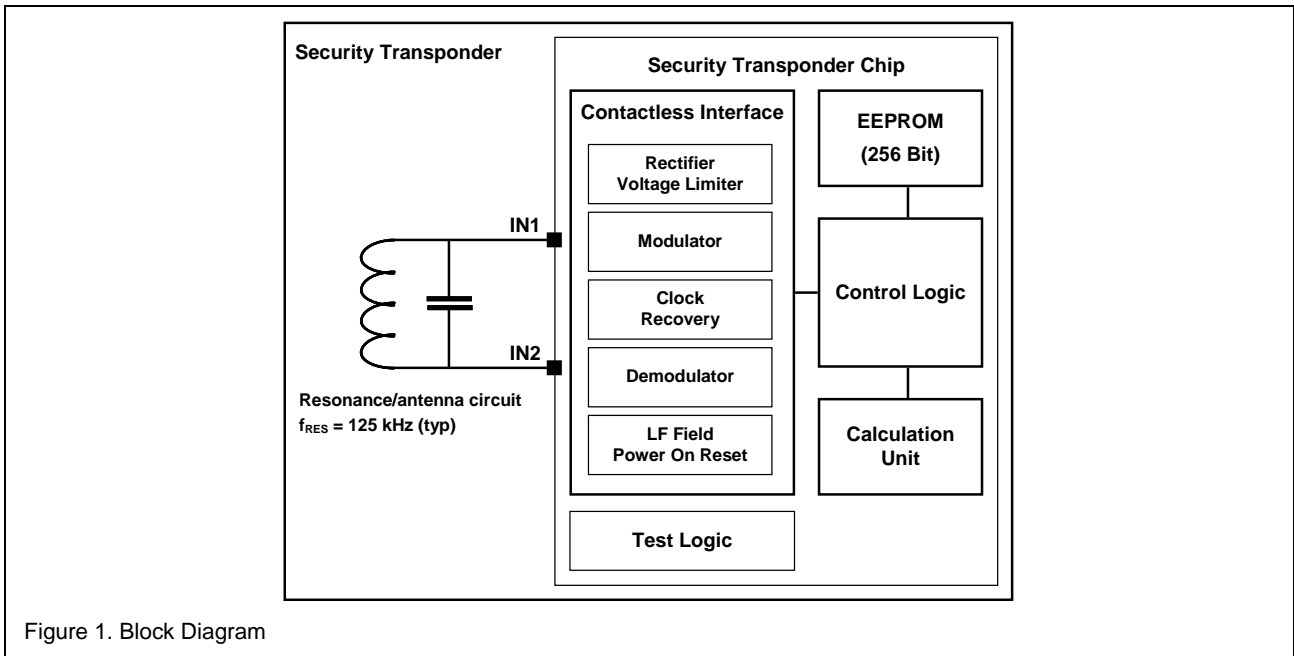


Figure 1. Block Diagram

5 TYPICAL APPLICATION

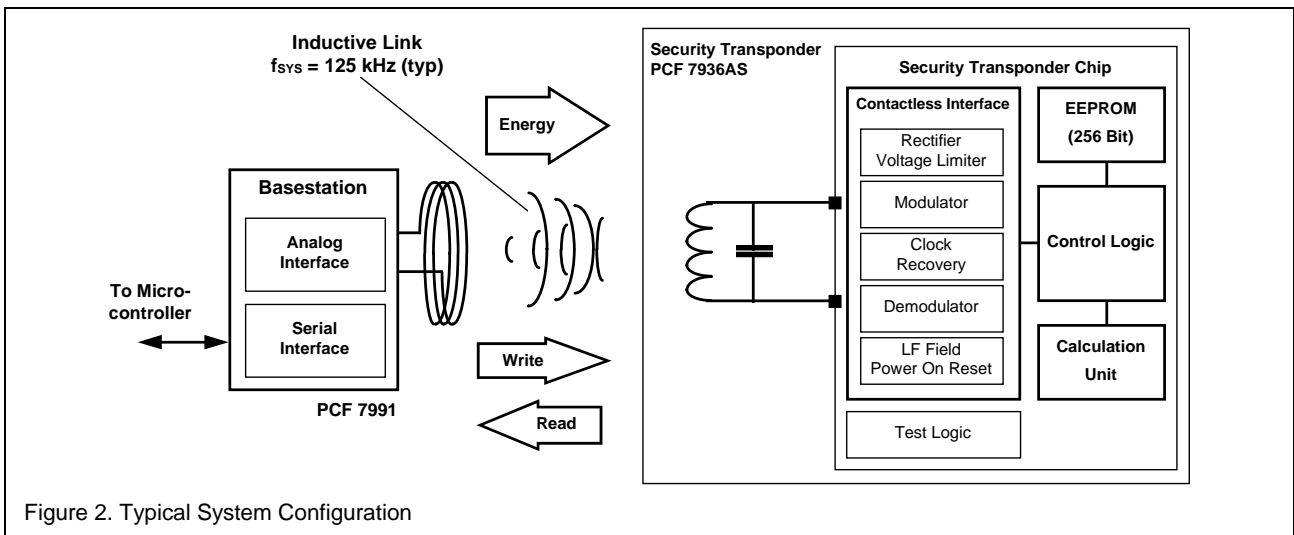


Figure 2. Typical System Configuration

Security Transponder (HITAG2)

PCF7936AS

6 QUICK REFERENCE DATA

PARAMETER	VALUE	UNIT
Carrier frequency	125	kHz
Data rate		
- read	4.0	kbit/s
- write	5.2	kbit/s
Data coding	Manchester or Bi-Phase Binary Pulse Length Modulation (BPLM)	
- read		
- write		
Data transmission mode	Half-Duplex	
Modulation	Amplitude Shift Keying (ASK)	
Memory size	256	bit
Identifier (serial number and product type ID)	32	bit
Secret Key (Cipher Mode)	48	bit
Password (Password Mode)	32	bit
Authentication time	39	ms
Special Features	<ul style="list-style-type: none"> • Ciphred mutual authentication • Ciphred data transmission • 128 bit user EEPROM with programmable write protection • Read/Write Password mode • Read Only emulation modes (H400x, ISO 11784/85 and PCF7931) 	

Security Transponder (HITAG2)

PCF7936AS

7 FUNCTIONAL DESCRIPTION SECURITY TRANSPONDER

The PCF7936AS does not require any additional power supply. It derives its power supply by inductive coupling to the LF Field, which is generated by the basestation. Reading and writing to the transponder is provided by amplitude modulation of the LF field.

The Contactless Interface generates the chip power supply, clock and reset and features the modulator, and demodulator. The system clock is derived from the LF field generated by the basestation that typically operates with a carrier frequency of 125 kHz.

The Control Logic incorporates the data acquisition logic to enable communication with the transponder and the memory access control logic. Access to the transponder memory (EEPROM) depends on the device configuration and the authentication state. The memory is split into blocks and pages with independent access rights, as configured by the user and partly predefined by design.

Device authentication may be performed in Password mode or in Ciphered mode. In Password mode the basestation and transponder in plain exchange a set of passwords, while in Cipher mode a mutual authentication based on a security algorithm is performed that employs a Secret Key and a random number. The security algorithm is determined by the on-chip Calculation Unit that in addition supports ciphered communication and data exchange between the basestation and the transponder.

The Cipher mode is ideally suited for vehicle immobilization application.

Transponder operation and authentication is controlled by commands send form the basestation, while in Read Only mode data transmission commences after device reset and a time-out condition.

7.1 Memory Organization, EEPROM

The device incorporates 256 bit of non-volatile memory (EEPROM) that is organized as 8 pages with 32 bit per page, referred to as Transponder Memory, TM. The Transponder Memory, TM, is split into areas for Transponder Configuration/Personalization, TCFG, and User Memory, USER, see Figure 3.

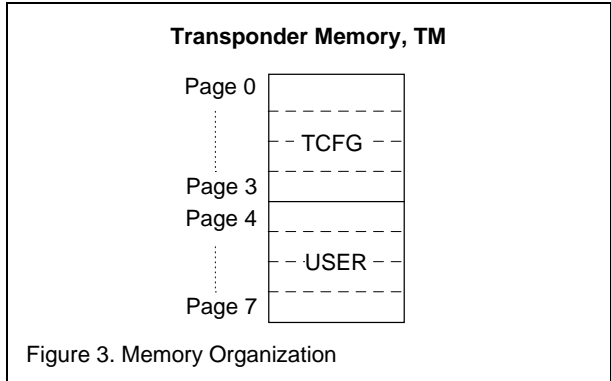


Figure 3. Memory Organization

The TM segment can be accessed only, after successful device authorization. Depending on the device configuration, device authorization is performed either in Password mode or in Cipher mode. Subsequent memory access is provided only in accordance with the memory protection settings applied.

Any changes made regarding the Transponder Configuration, TCFG, respectively Page 1 to 3, become effective after a device reset or initialization sequence only.

The organization of the Transponder Memory, TM, depends on the authorization method selected (Password or Cipher mode) by the corresponding configuration bit (ENC) see Figure 4.

Security Transponder (HITAG2)

PCF7936AS

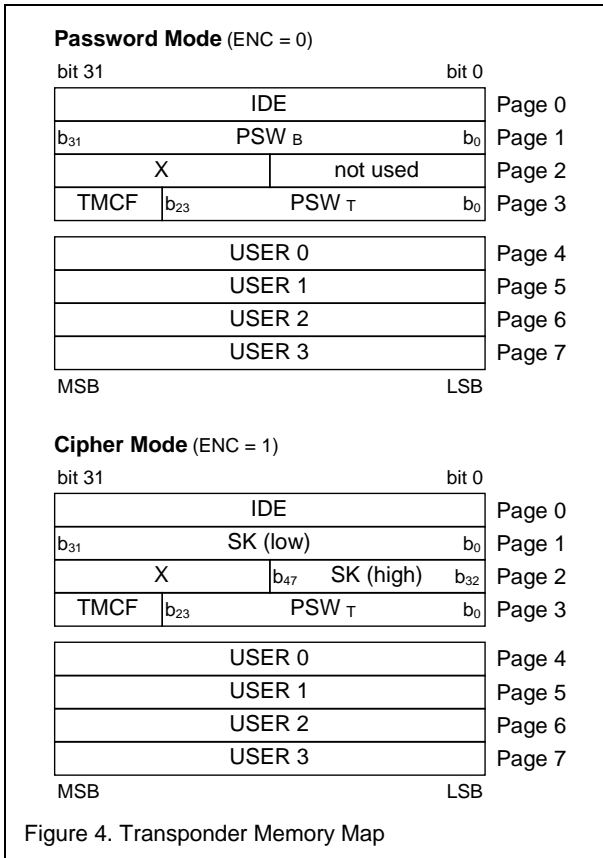


Figure 4. Transponder Memory Map

Note

- Locations marked 'X' are for device internal use. They are partly initialized and locked against overwriting during device manufacturing and are not available for data storage. Any read operation yields an undefined bit value.

Pages 0 to 3 of the EEPROM memory are reserved for transponder configuration and personalization, while Page 4 to 7 are reserved for user data storage, USER.

According to the selected authorization method, page 1 and 2 do hold a Password, PSW_B, (Password mode) or the Secret Key, SK, (Cipher mode).

7.1.1 Identifier, IDE

The Identifier, IDE, is a factory programmed quasi unique 32 bit pattern that serves the function of a device serial number (SN) and product type identification (PI). The Identifier is located in page 0 and supports read access only, thus cannot be altered.

The product type identification is located in the bits 4 to 7 and factory programmed for all PCF7936AS devices to 1_H, as shown in Figure 5.

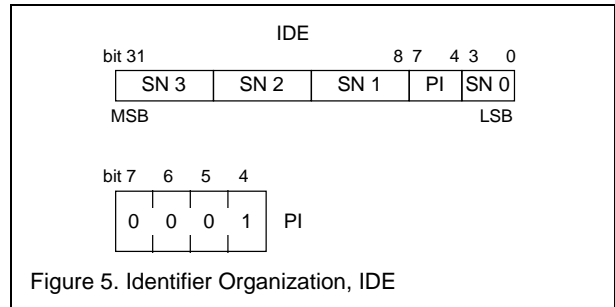


Figure 5. Identifier Organization, IDE

The Identifier, IDE, is transmitted in plain and incorporated in the process of device authentication, thus used by the on-chip Calculation Unit as well as by the interrogating system.

7.1.2 Password Basestation, PSW_B

The Password Basestation, PSW_B, is applicable in Password mode only (ENC = 0). The Password Basestation is a 32 bit pattern, which typically is initialized and subsequently locked by the customer during device personalization. The Password Basestation is located in page 1, see Figure 4.

During the process to identify the basestation towards the transponder, the transponder verifies the password received by the basestation with the password stored in PSW_B. If both match each other, the transponder assumes successful identification of the basestation and the authentication sequence is continued, otherwise it is terminated. For details refer to section 7.3.1, START_AUTH command.

The Password Basestation may be assigned any value that is considered useful by the application. The PSW_B can be protected against reading and writing by setting the lock bit SKL, see section 7.1.4

NXP initializes the Password Basestation with a common Transport Key value as specified (see section 8), in order to enable initial device access. Since the corresponding lock bit is not set, the PSW_B Transport Key value and device configuration can be read and modified at any time as desired.

Security Transponder (HITAG2)

PCF7936AS

7.1.3 Secret Key, SK

The Secret Key, SK is applicable in Cipher mode only (ENC = 1). The Secret Key is a 48 bit pattern, which typically is initialized and subsequently locked by the customer during device personalization. The Secret Key is located in page 1 and 2, see Figure 4.

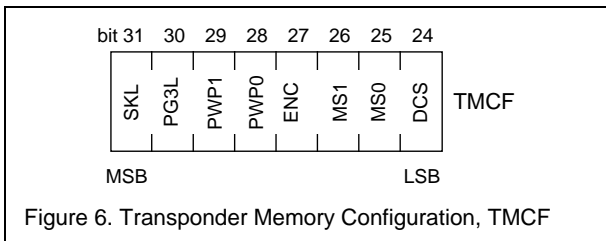
The 32 least significant bits of SK (bit 31 to bit 0) are located in page 1 while the 16 most significant bits (bit 47 to bit 32) are located in page 2 at bit address 0 to 15.

The Immobilizer Secret Key is incorporated in the process of device authentication and used by the on-chip calculation unit as well as by the interrogating system. However the Immobilizer Secret Key is never transmitted during the process of device authentication. For details refer to section 7.3.1, START_AUTH command.

The Secret Key may be assigned any value that is considered useful by the application. The SK can be protected against reading and writing by setting the lock bit SKL, see section 7.1.4

7.1.4 Transponder and Memory Configuration, TMCF

Access to the Transponder Memory, TM, and device configuration is controlled by a set of configuration bits, TMCF, located in page 3, see Figure 6.



The memory access rights applied by TMCF affect the behavior of READ_PAGE and WRITE_PAGE commands only. Device operation, e.g. with respect to the authentication process, is not affected at all.

Secret Key Lock, SKL

If set, the Password Basestation, PSW B, (Password mode) or the Secret Key, SK, (Cipher mode) is irreversible locked against reading and writing (OTP like). If set once, its value can no longer be read or altered.

Page 3 Lock, PG3L

If set, page 3 is irreversible locked against writing (OTP like). Thus if set once, the Transponder and Memory Configuration (TMCF) as well as the Password Transponder (PSW T) can no longer be altered. However, reading is supported in any case.

Protect Write User Page 4 and 5, PWP1

If set, a write protection is assigned for the user pages page 4 and 5 (USER0 and USER1). As a result its content cannot be altered, however, reading is supported in any case.

If cleared, page 4 and page 5 support reading and writing.

The content and organization of the user pages is fully determined by the application.

Protect Write User Page 6 and 7, PWP0

If set, a write protection is assigned for the user pages page 6 and 7 (USER2 and USER3). As a result its content cannot be altered, however, reading is supported in any case.

If cleared, page 6 and page 7 support reading and writing.

The content and organization of the user pages is fully determined by the application.

Enable Cipher Mode, ENC

The device may be configured for to perform authentication in either Password mode or Cipher mode.

If ENC is set, Cipher mode is selected, otherwise Password mode.

Thus, ENC affects operation of the START_AUTH command and whether plain or ciphered transmission of data and commands is supported, for details refer to section 7.3.1.

Security Transponder (HITAG2)

PCF7936AS

Mode Select, MS

The device may be configured for to support one out of three Read Only modes, which will cause the device to commence data transmission after the specified time-out period, without interrogation by the basestation, see Table 1.

Table 1. Mode Select

MS1	MS0	Read Only Mode	Note
0	0	ISO 11784/5	
0	1	MIRO	1
1	0	PCF7931/30/35	2
1	1	Disabled	

Note

1. Emulates MIRO and H400x like Read Only transponders
2. Features compatibility with NXP' PIT family operated in Read Only mode, except for the PMC timing (Program Mode Check) and available memory size.

For details regarding the timing and sequence transmitted refer to section 7.5.

If MS is set, the device does not support Read Only operation at all.

Data Coding Select, DCS

In Password or Cipher mode data transmitted from the transponder to the basestation may be encoded in Manchester or CDP fashion, according to the setting of DCS.

If DCS is cleared, Manchester encoding is applied, otherwise CDP coding is applied, see section 7.6.1 for details.

However, if the device operates in one of the Read Only modes, data transmission and encoding corresponds to the Read Only mode selected and is not affected by DCS at all, see section 7.5 for details.

7.1.5 Password Transponder, PSW_T

The Password Transponder, PSW_T, is a 24 bit pattern, which typically is initialized and subsequently locked by the customer during device personalization. The Password Transponder is located in page 3, see Figure 4.

The Password Transponder serves the function to identify the transponder towards the basestation. After successful device authentication, the transponder returns the content of page 3 to the basestation. In Password mode the content is returned in plain, while in Cipher mode the content is returned in ciphered fashion. For details refer to section 7.3.1, START_AUTH command.

Thus the Password Transponder and TMCF configuration may be evaluated by the basestation, if desired. The Password Transponder may hold any value that is considered useful by the application.

7.1.6 User Pages, USER 0 to 3

Page 4 to 7 provide space for user data storage. Data access is supported according to the device configuration selected.

The user pages may hold any data that is considered useful by the application.

Security Transponder (HITAG2)

PCF7936AS

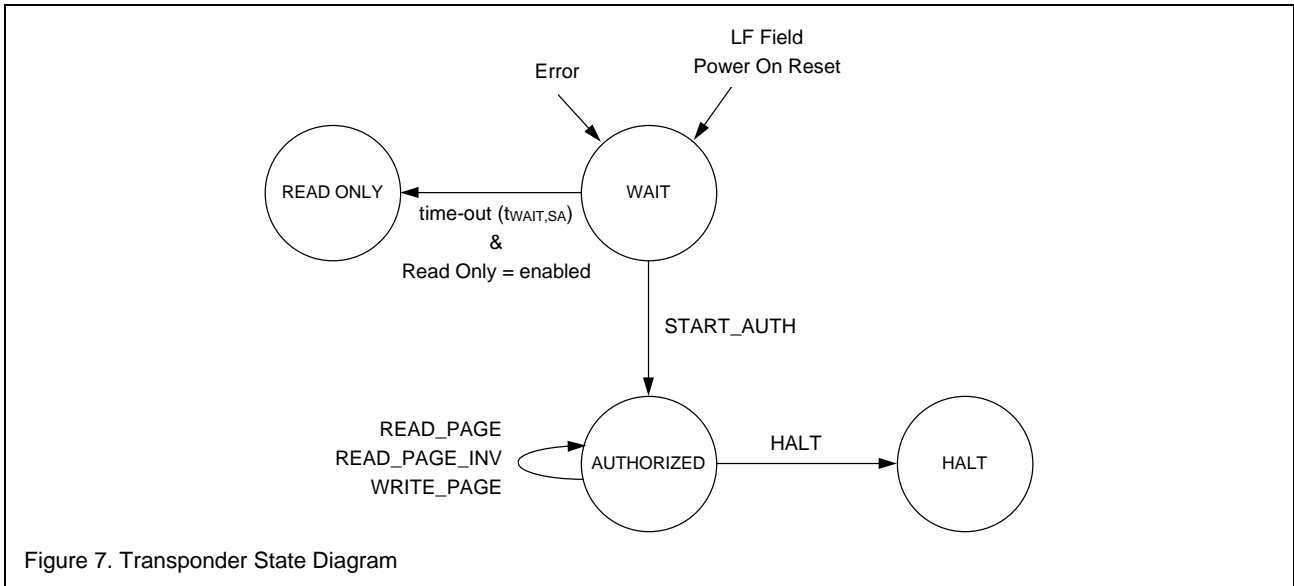


Figure 7. Transponder State Diagram

7.2 Transponder State Diagram

Device operation is controlled by commands issued from the basestation, see Figure 7.

After a LF Field Power-On Reset condition the circuitry is reset and the transponder is initialized, which causes the device to enter the WAIT state.

If one of the Read Only modes is enabled, the device will enter READ ONLY state after the specified time-out ($t_{WAIT,SA}$), if no command is being issued.

To authenticate the transponder and to access the Transponder Memory for read and write the AUTHORIZED state has to be entered, by means of a START_AUTH command and successful completion of the authentication sequence. Subsequent memory read and write operations may be executed.

Operation of the transponder commands depend on the device configuration (Password or Cipher Mode).

If the device is forced into HALT state, by means of the HALT command, the transponder circuitry is muted.

A violation of the command sequence coding or command timing in any state causes an error condition, which causes the device to enter WAIT state and to reset the time-out ($t_{WAIT,SA}$).

7.2.1 WAIT State

In WAIT state general memory access is denied. Commands may be issued to start device authentication, in order to enter the AUTHORIZED state, see Table 2.

Table 2. Command Set in WAIT State

NAME	COMMAND, CMD				
	CM4	CM3	CM2	CM1	CM0
Reserved ¹⁾	0	X	X	X	X
Reserved ¹⁾	X	0	X	X	X
Reserved ¹⁾	X	X	1	X	X
Reserved ¹⁾	X	X	X	1	X
Reserved ¹⁾	X	X	X	X	1
START_AUTH	1	1	0	0	0

Note

1. This command is reserved for future use and subject to change without notice. The actual implementation causes the device to generate an error condition and to enter the WAIT state, if this command is being issued.

Upon entering the WAIT state the time-out ($t_{WAIT,SA}$) is reset. In case $t_{WAIT,SA}$ is allowed to time-out, the device enters READ ONLY state, if one of the Read Only modes is enabled. In case a START_AUTH command is issued, device authentication is triggered and the READ ONLY state is not entered. At least the first two bits of START_AUTH need to be recognized by the device within the time-out period specified by $t_{WAIT,SA}$.

Security Transponder (HITAG2)

PCF7936AS

7.2.2 AUTHORIZED State

The AUTHORIZED state is entered only after successful device authentication, see START_AUTH command. In AUTHORIZED state the Transponder Memory, TM, can be accessed by means of subsequent read and write commands, see Table 3.

Communication with the device employs plain (Password Mode) respectively ciphered (Cipher Mode) transmission of commands and data.

The Transponder Memory is accessed page wise in accordance with the memory protection configuration.

Table 3. Command Set in AUTHORIZED State

NAME	COMMAND, CMD				
	CM4	CM3	CM2	CM1	CM0
READ_PAGE	1	1	pg2	pg1	pg0
READ_PAGE_INV	0	1	pg2	pg1	pg0
WRITE_PAGE	1	0	pg2	pg1	pg0
HALT ¹⁾	0	0	X (0)	X (0)	X (1)

Note

- Any coding of the bits CM[2:0] will force HALT state, however, for future compatibility the values in brackets should be applied.

Any read respectively write attempt to a page that is read respectively write protected by the corresponding bit in the configuration page, would cause the device to terminate the AUTHORIZED state and to enter WAIT state.

7.2.3 HALT State

The HALT state may be entered from AUTHORIZED state only. In HALT state the device is muted and any further commands are ignored.

To exit the HALT state a transponder LF Field Power-On Reset condition must be generated, by means of muting the LF field for the specified time.

7.2.4 READ ONLY State

The READ ONLY state is entered without command interrogation, after termination of the time-out, $t_{\text{WAIT,SA}}$, see also section 7.7.

In READ ONLY mode command decoding is disabled and the device repeatedly transmits user data, according to the selected Read Only mode, see section 7.5.

The READ ONLY state may be terminated as a result of a transponder LF Field Power-On Reset condition only, by means of muting the LF field for the specified time.

Security Transponder (HITAG2)

PCF7936AS

7.3 Command Set

Device operation is controlled by commands issued from the basestation. Table 4 gives a comprehensive summary of the applicable commands in alphabetic order. Command

operation and acceptance depend on the actual device state in which the command is being issued as well as on the device configuration (Password/Cipher Mode), see also section 7.2. A command being issued in a different state may cause an error condition.

Table 4. Command Set Summary

NAME	DESCRIPTION	APPLICABLE DEVICE STATE
HALT	Forces the device to enter the HALT state	AUTHORIZED
READ_PAGE	Reads 32 bit from the designated memory page, if not restricted by the corresponding memory protection flags or by specification	AUTHORIZED
READ_PAGE_INV	Reads 32 bit from the designated memory page, if not restricted by the corresponding memory protection flags or by specification. The content of the page is returned in inverse polarity.	AUTHORIZED
START_AUTH	Starts the device authentication sequence	WAIT
WRITE_PAGE	Writes 32 bit to the designated memory page, if not restricted by the corresponding memory protection flags or by specification	AUTHORIZED

Security Transponder (HITAG2)

PCF7936AS

7.3.1 Command Description

The general form of a control sequence consists of the command sequence send to the transponder and an Equalizer pattern (EQ) and Response received from the transponder. The general control sequence timing is shown in Figure 8.

When switching from SEND to RECEIVE and vice versa, the basestation and control software have to consider the indicated delays ($t_{WAIT,Tr}$ and $t_{WAIT,Bs}$), during which the basestation must not transmit any data or commands.

Depending on the command, the Command Sequence consists of a minimum of 5 bit respectively 10 bit. For data integrity reasons memory read and write commands have to be transmitted in normal coding and in inverted coding before being accepted by the device, which yields a minimum Command Sequence of 10 bit.

The Equalizer, EQ, consist of a 5 bit pattern (all ones) for basestation settling and software synchronization purposes. The device response consists of a command acknowledgment and/or the requested data.

Some operations require additional parameter to be send to and/or to be received from the device, e.g. WRITE_PAGE or START_AUTH.

For proper operation, command execution by the device must not be suspended for more than the specified Idle time (t_{IDLE}), see Figure 9. Otherwise the device may stop command decoding, disabling any communication with the device. In this case, a LF Field Power-On Reset has to be applied, in order to reset and initialize the circuitry, see section 7.7. Consequently, the device resumes WAIT state. As indicated, the Idle time is specified as the time interval between the last bit received from the transponder and the last bit of the Command Sequence send to the transponder. Some commands allow repeating the command several times for data integrity reasons, however, in any case the limitations imposed by the Idle time have to be considered.

The Idle time applies also for the very first command send to the device after a device LF Field Power-On Reset condition, see also section 7.7.

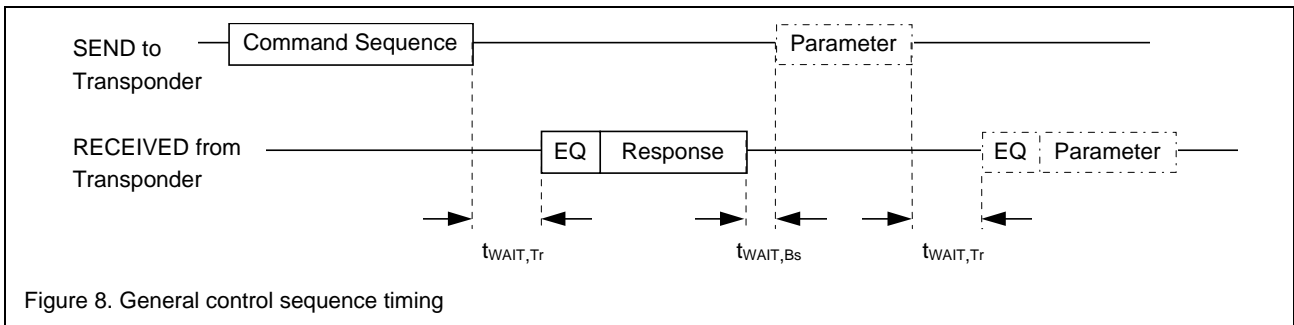


Figure 8. General control sequence timing

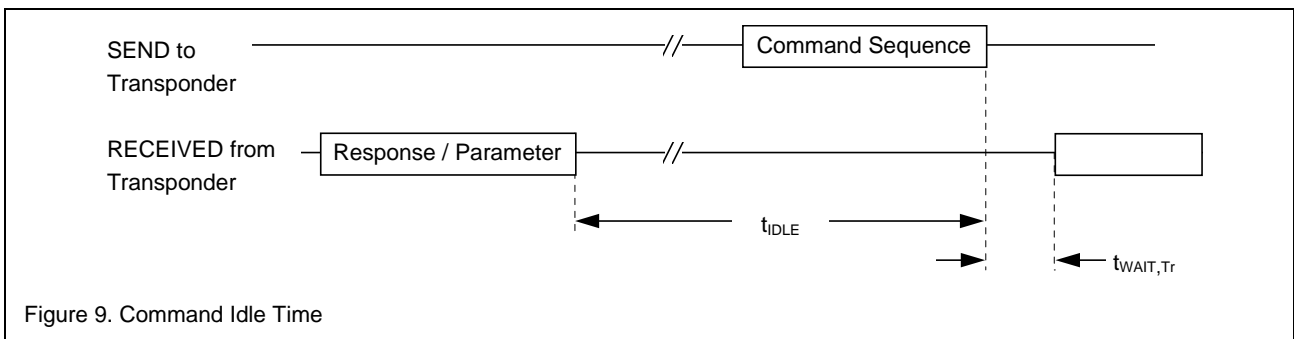


Figure 9. Command Idle Time

Security Transponder (HITAG2)

PCF7936AS

HALT

The command HALT may be issued in AUTHORIZED state and forces the device to enter the HALT state. For data integrity reasons the 5 bit command and its complement have to be send, before the device will accept it, see Figure 10. If accepted, the command Response consist of the command itself and its complement.

The 10 bit command sequence may be repeated several times, if desired, to increase the data integrity level. In the case that one of the 5 bit commands and its complement do not match, an error condition occurs that causes the device to terminate the command, to initialize the device and to enter the WAIT state. No command Response will be send by the device in this case.

If the device is configured for Password mode (ENC = 0) the command sequence is transmitted in plain, while in Cipher mode (ENC = 1) the whole command sequence is transmitted ciphered.

READ_PAGE

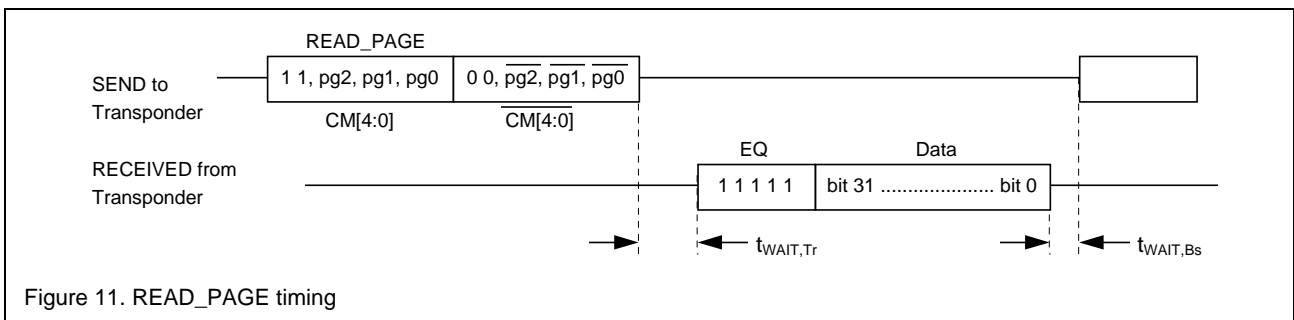
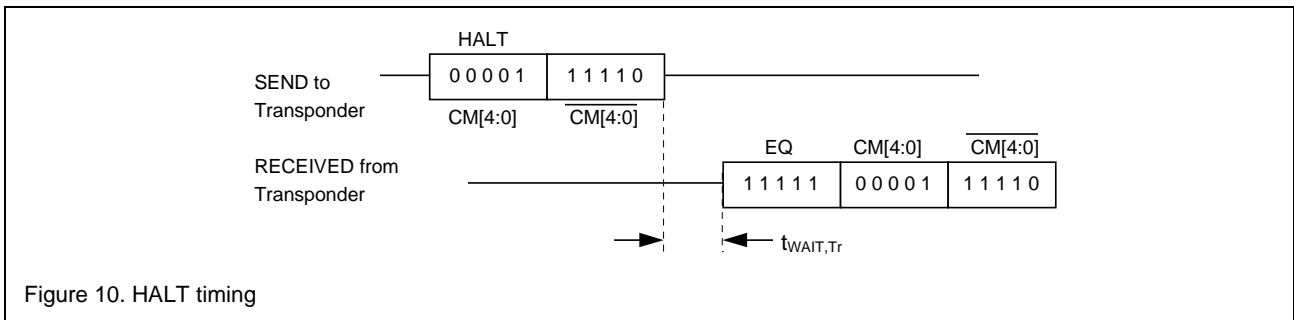
The command READ_PAGE returns the content of the designated page. The page designated for reading is specified by the command bits pg2 to pg0. For data integrity reasons the 5 bit command and its complement have to be send, before the device will accept it, see Figure 11. If accepted, the command Response consists of the 32 bit content of the designated page. The MSB is send first.

The 10 bit command sequence may be repeated several times, if desired, to increase the data integrity level. In the case that one of the 5 bit commands and its complement do not match, an error condition occurs that causes the device to terminate the command, to initialize the device and to enter the WAIT state. No command Response will be send by the device in this case.

Subsequent commands may be issued after termination of $t_{WAIT,Bs}$.

Any attempt to read a page that is protected against reading, will be detected and cause an error condition, upon which the device terminates the command during $t_{WAIT,Tr}$ and enters the WAIT state. No Response will be send in this case.

If the device is configured for Password mode (ENC = 0) the command sequence is transmitted in plain, while in Cipher mode (ENC = 1) the whole command sequence is transmitted ciphered.



Security Transponder (HITAG2)

PCF7936AS

READ_PAGE_INV

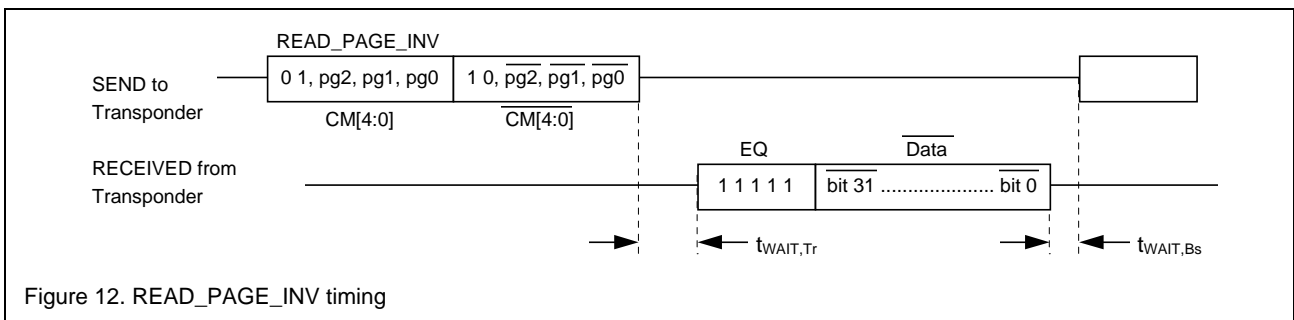
The command READ_PAGE_INV returns the complement of the content of the designated page. The page designated for reading is specified by the command bits pg2 to pg0. For data integrity reasons the 5 bit command and its complement have to be send, before the device will accept it, see Figure 12. If accepted, the command Response consists of the complement of the 32 bit content. The MSB is send first.

The 10 bit command sequence may be repeated several times, if desired, to increase the data integrity level. In the case that one of the 5 bit commands and its complement do not match, an error condition occurs that causes the device to terminate the command, to initialize the device and to enter the WAIT state. No command Response will be send by the device in this case.

Subsequent commands may be issued after termination of $t_{WAIT,Bs}$.

Any attempt to read a page that is protected against reading, will be detected and cause an error condition, upon which the device terminates the command during $t_{WAIT,Tr}$ and enters the WAIT state. No Response will be send in this case.

If the device is configured for Password mode (ENC = 0) the command sequence is transmitted in plain, while in Cipher mode (ENC = 1) the whole command sequence is transmitted ciphered.



Security Transponder (HITAG2)

PCF7936AS

START_AUTH (Password Mode)

If configured for Password mode, START_AUTH triggers the mutual device authentication sequence. If completed successfully, the device enters AUTHORIZED state and subsequently supports plain read and write access of the Transponder Memory, TM. Device authentication employs the Password Basestation, PSW_B, and Password Transponder, PSW_T, see Figure 13.

After acceptance of the 5 bit command sequence, the initial device Response consist of the 32 bit Identifier (IDE) that is stored in the Transponder Memory. Subsequently, the interrogating system (e.g. basestation) has to identify itself towards the device, by issuing the matching 32 bit Password Basestation, PSW_B. The device verifies the Password received with the one stores in the page 1. If identical, the final device Response consist of the content of page 3 that contains the Transponder and Memory configuration (TMCF) and device Password Transponder (PSW_T). The MSB is send first.

In case the authentication process fails, an error condition occurs that causes the device to terminate the command and to enter WAIT state. The device will send no further Response in this case.

Subsequent commands may be issued after termination of the final $t_{WAIT,BS}$.

For proper command execution, the interrogating system has to identify itself towards the device within the specified IDLE time, otherwise the device may generate a power-on reset condition, upon which the circuitry would be reset and the transponder initialized, causing the device to enter the WAIT state.

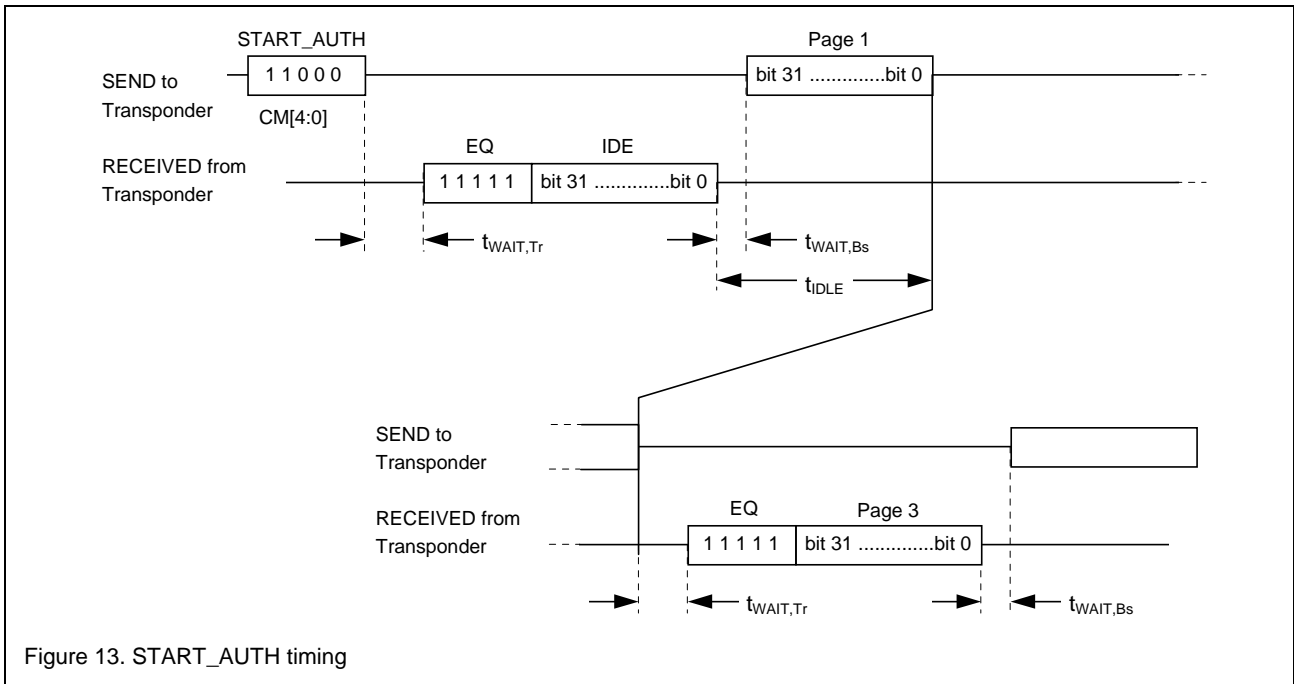


Figure 13. START_AUTH timing

Security Transponder (HITAG2)

PCF7936AS

START_AUTH (Cipher Mode)

If configured for Cipher mode, START_AUTH triggers the mutual device authentication sequence. If completed successfully, the device enters AUTHORIZED state and subsequently supports ciphered read and write access of the Transponder Memory, TM. Device authentication employs the Identifier, a Random Number, a ciphered Signature and a ciphered device Response, see Figure 13.

After acceptance of the 5 bit command sequence, the initial device Response consist of the 32 bit Identifier (IDE) that is stored in the Transponder Memory. Subsequently, the interrogating system (e.g. basestation) has to identify itself towards the device, by issuing a 32 bit Random Number and a matching 32 bit ciphered Signature. The device verifies the authenticity of the ciphered Signature received, by means of the Calculation Unit, involving the Secret Key (SK). If successful, the final device Response consists of the ciphered content of page 3 that contains the Transponder and Memory configuration (TMCF) and device Password Transponder (PSW_T). The MSB is send first.

In case the authentication process fails, an error condition occurs that causes the device to terminate the command and to enter WAIT state. The device will send no further Response in this case.

Subsequent commands may be issued after termination of the final $t_{WAIT,BS}$.

For proper command execution, the interrogating system has to identify itself towards the device within the specified IDLE time, otherwise the device may generate a power-on reset condition, upon which the circuitry would be reset and the transponder initialized, causing the device to enter the WAIT state.

The Security Algorithm details, involved in the process of mutual device authentication, are specified in a separate Application Note. Please contact your NXP representative for more information.

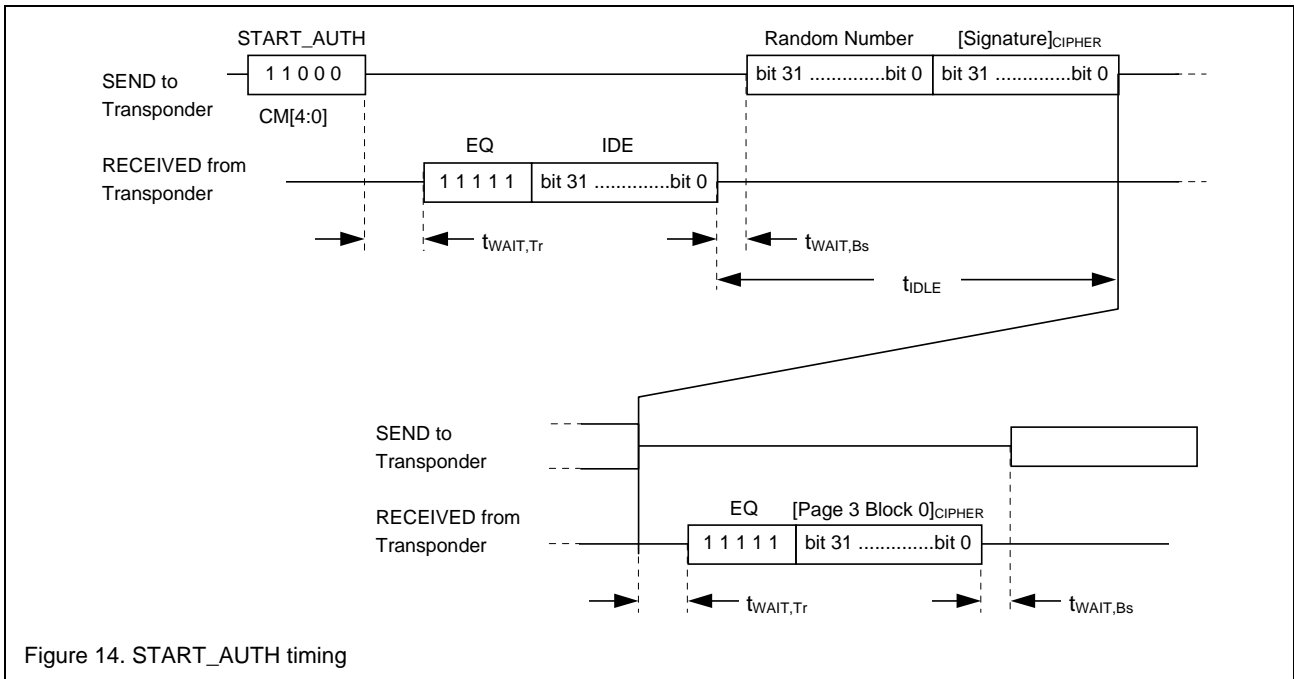


Figure 14. START_AUTH timing

Security Transponder (HITAG2)

PCF7936AS

WRITE_PAGE

The command WRITE_PAGE writes the data supplied with this command into the designated page. The page designated for writing is specified by the command bits pg2 to pg0. For data integrity reasons the 5 bit command and its complement have to be send, before the device will accept it, see Figure 15. If accepted, the command Response consist of the command itself, and the corresponding complement.

The 10 bit command sequence may be repeated several times, if desired, to increase the data integrity level. In the case that one of the 5 bit commands and its complement do not match, an error condition occurs that causes the device to terminate the command, to initialize the device and to enter the WAIT state. No command Response will be send by the device in this case nor does the designated page being overwritten.

After termination of t_{PROG} the device checks, if the EEPROM write operation completed successfully, if not, an error condition occurs that causes the device to enter the WAIT state.

In the case the write operation did not complete successfully, the designated EEPROM page may hold an undefined content or may suffer from a weak programming.

In order to unambiguously verify, whether programming of the designated page completed properly, the basestation has to identify, if the device still resides in AUTHORIZED state or entered WAIT state. Thus, a READ_PAGE or READ_PAGE_INV command should be issued subsequently and monitored, if this command executes properly.

If the device still resides in AUTHORIZED state, command execution would complete successfully and after verifying the data that has been read, proper operation of the corresponding WRITE_PAGE command can be assumed.

Subsequent commands may be issued after termination of the final $t_{WAIT,Bs}$.

Any attempt to write a page that is protected against overwriting will be detected and cause an error condition, upon which the device terminates the command during $t_{WAIT,Tr}$ and enters the WAIT state. No Response will be send in this case.

If the device is configured for Password mode (ENC = 0) the command sequence is transmitted in plain, while in Cipher mode (ENC = 1) the whole command sequence is transmitted ciphered.

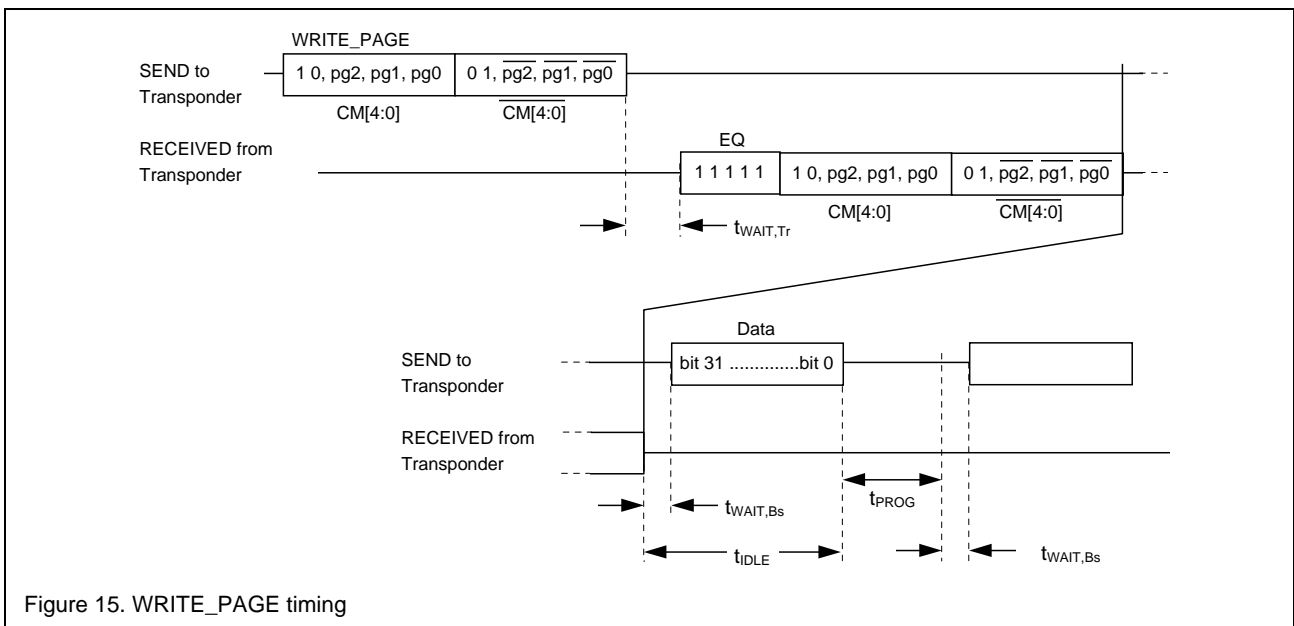


Figure 15. WRITE_PAGE timing

Security Transponder (HITAG2)

PCF7936AS

7.4 Calculation Unit

The PCF7936AS incorporates a Calculation Unit for use during mutual device authentication, command operation and EEPROM data exchange, if the device is configured for Cipher mode. The security algorithm involves a quasi unique 32 bit Identifier, a 48 bit Secret Key and a 32 bit Random Number.

The Identifier and the Secret Key are stored in the Transponder Memory, TM. The Identifier (IDE) is a factory programmed quasi unique pattern, while the Secret Key is initialized and subsequently locked by the customer during device personalization.

Mutual authentication of the Security Transponder in Cipher mode is triggered by means of the START_AUTH command, see also section 7.3. As a result, the device reveals its Identifier to the interrogating system (basestation) and subsequently the interrogating system has to send a 32 bit Random Number and a ciphered Signature to the device. Both are processed by the Calculation Unit, involving the Secret Key (SK) and Identifier (IDE), in order to authenticate the interrogating system. If successful, the device replies with a ciphered response for validation by the interrogating system.

Details concerning the security algorithm implementation are specified in a separate Application Note. Please contact your local NXP representative for more information.

Security Transponder (HITAG2)

PCF7936AS

7.5 Read Only Modes

If the device is configured for one of three Read Only modes, it will cyclically transmit data while operating in READ ONLY state. The corresponding Read Only mode is selected by the configuration bit MS1 and MS0, located in the EEPROM, see section 7.1.4.

In Read Only mode, the data rate and coding is fixed as specified and cannot be altered for the corresponding mode. Data is transmitted until an LF Field Power-On Reset terminates the READ ONLY state.

7.5.1 ISO 11784/5 (MS1 = 0, MS0 = 0)

If the Read Only mode ISO 11784/85 is selected, the device cyclically transmits user page 4 to 7, see Figure 16.

The rate is fixed to 32 T_O per bit ($T_{BIT} = 32 T_O$) and CDP encoding is applied.

7.5.2 MIRO Mode (MS1 = 0, MS0 = 1)

If the Read Only mode MIRO is selected, the device cyclically transmits user page 4 to 5, see Figure 17.

The rate is fixed to 64 T_O per bit ($T_{BIT} = 64 T_O$) and Manchester encoding is applied.

7.5.3 PCF7931/30/35 (MS1 = 1, MS0 = 0)

If the Read Only mode PCF7931/30/35 is selected, the device cyclically transmits user page 4 to 7, while inserting a PMC pattern, as known from the PIT transponder family (PCF7931/30), see Figure 18.

However, the modified PMC pattern implemented for the PCF7936AS does not fully comply with the one used for the PIT family.

The rate is fixed to 64 T_O per bit ($T_{BIT} = 64 T_O$) and CDP encoding is applied.

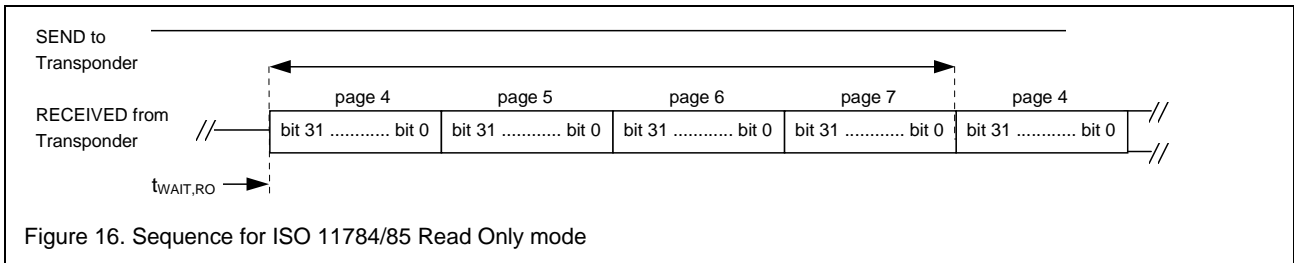


Figure 16. Sequence for ISO 11784/85 Read Only mode

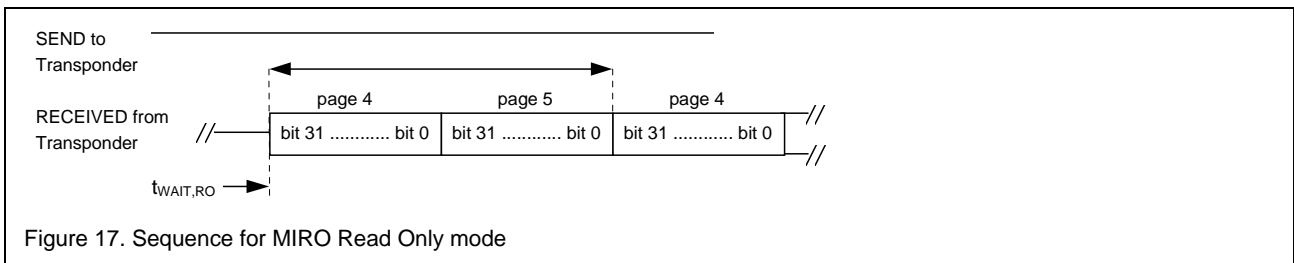


Figure 17. Sequence for MIRO Read Only mode

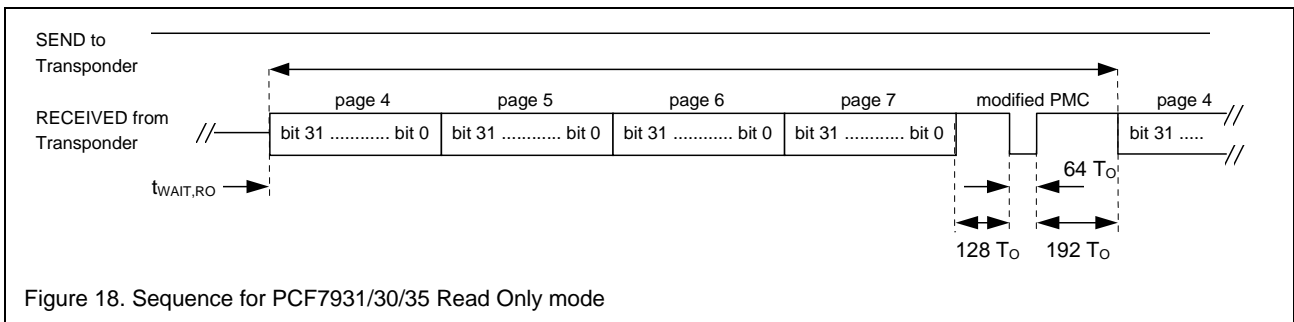


Figure 18. Sequence for PCF7931/30/35 Read Only mode

Security Transponder (HITAG2)

PCF7936AS

7.6 Transponder Data Transmission Format

Reading from and writing to the device is accomplished by modulating the LF field in amplitude. Since the LF field also provides the device power supply, the modulation characteristics have to be verified carefully, in order to avoid a device reset due to a power low condition.

7.6.1 Read Direction

Transmission of data from the transponder to the basestation is accomplished by absorption modulation applied to the LF field. According to the data designated for transmission, the transponder interface activates an additional load that modulates the current drawn from the transponder resonant circuit. Due to the inductive coupling of the transponder resonant circuit and the basestation coil, the current in the basestation coil is modulated accordingly, resulting in a corresponding two-level amplitude modulation, see Figure 19.

In read direction the device employs either Manchester or CDP encoding of data, see Figure 20, according to the

setting of the Immobilizer Configuration bit DCS, which is part of the Transponder and Memory Configuration bits, TCMF, see also section 7.1.4.

In case of Manchester encoding, a logic '1' is modulated by loading the LF field during the first half of the bit frame, while no load is applied during the second half. A logic '0' is modulated in the opposite manner.

In case of CDP encoding, a logic '1' corresponds to a state change at the end of the bit frame. A logic '0' corresponds to a state change after the first half and at the end of the bit frame.

In any case, the device starts with a „Load ON“ condition, when data transmission commences.

The bit duration is a fixed multiple of the system clock recovered from the LF field carrier.

After reception of the last bit, the basestation and control software have to consider the indicated delay, $t_{WAIT,Bs}$, before any command or data is transmitted to the device, see also section 7.3.1.

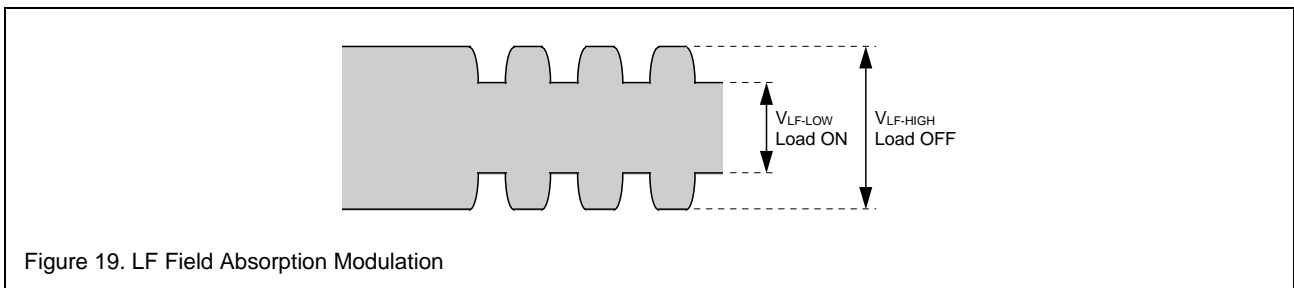


Figure 19. LF Field Absorption Modulation

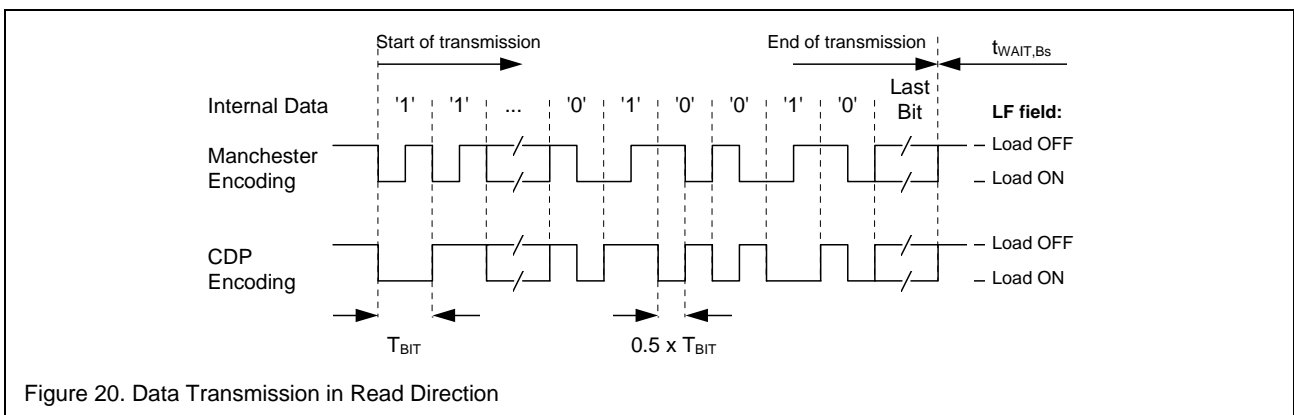


Figure 20. Data Transmission in Read Direction

Security Transponder (HITAG2)

PCF7936AS

7.6.2 Write Direction

Transmission of data from the basestation to the transponder is accomplished by Amplitude Shift Keying (ASK) of the LF field with a modulation index as specified. According to the data designated for transmission, the basestation coil driver is simply switched ON and OFF (tri-state) typically. Due to the inductive coupling of the transponder resonant circuit and the basestation coil, the voltage of the transponder resonant circuit is modulated accordingly. Resulting in a two-level amplitude modulation that is detected by the transponder interface demodulator circuitry, see Figure 21.

The PCF7936AS transponder demodulator circuitry has been optimized for basestations with antenna coil drivers that perform the LF field modulation by Tri-State switching of the driver stage.

In write direction Binary Pulse Length Modulation (BPLM) is applied for data encoding, see Figure 22.

Sending data or commands to the device commences with an initial write pulse that marks transmission start. A logic '0' or '1' is signaled to the transponder by the corresponding repetition time (T_{LOG_0} respectively T_{LOG_1}) of the write pulse sequence.

The end of the transmitted bit string is marked by a stop condition. A stop condition is detected by the transponder, if no write pulse is detected for the specified time (T_{STOP}).

In the case the bit string transmitted causes the device to respond with data, modulation of the LF field by the device does commence after the specified time out ($t_{WAIT,Tr}$), see also section 7.3.1.

Violation of the specified timing causes an error condition, upon which the device enters the WAIT state, see also section 7.2.

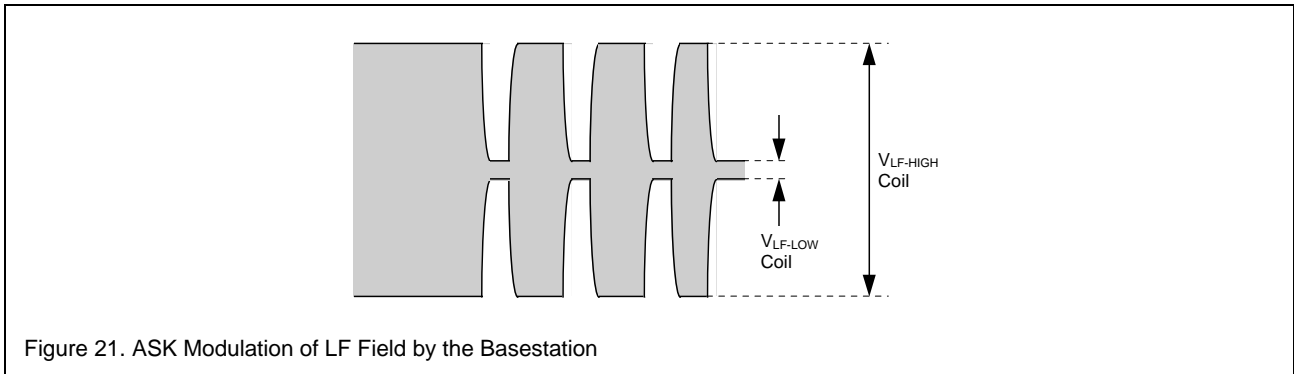


Figure 21. ASK Modulation of LF Field by the Basestation

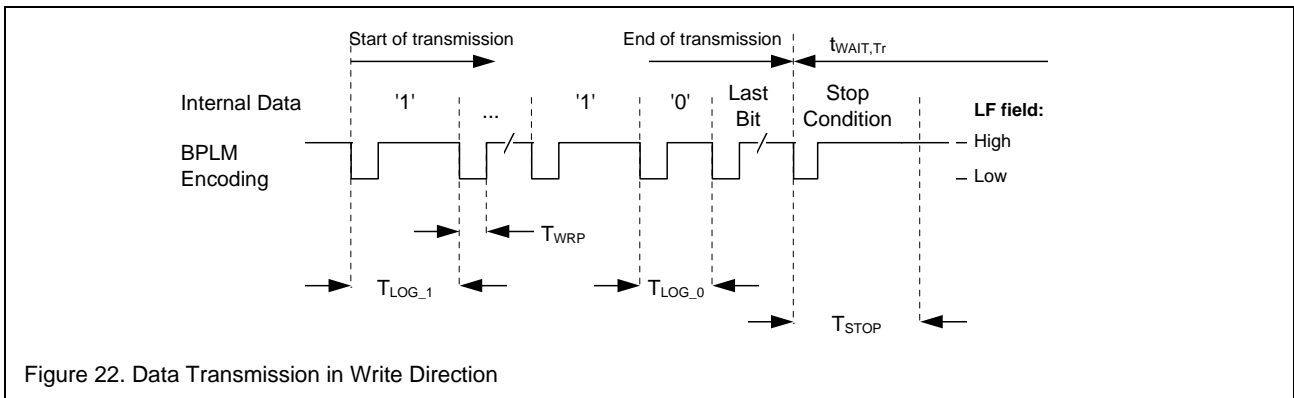


Figure 22. Data Transmission in Write Direction

Security Transponder (HITAG2)

PCF7936AS

7.7 LF Field Power On Reset

When the transponder enters a LF field a rectifier circuitry becomes operational and the internal transponder supply voltage (V_{DD}) develops. As soon as the supply voltage exceeds the LF Field Power-On Reset threshold voltage (V_{THR}) the device performs a chip reset and starts its initialization sequence, see Figure 23.

Subsequently, the transponder is muted and does not respond to any command prior to termination of the initialization sequence, t_{INIT} . The startup time, t_{START} , depends on the basestation configuration, the resonance circuit properties and the system coupling factor, however, is small compared with the initialization time typically.

For proper device operation, after a LF Filed Power-On Reset condition, command execution must commence within the specified Idle time, t_{IDLE} , see Figure 23. Otherwise the device may stop command decoding, disabling any communication with the device. In this case a

LF Field Power-On Reset has to be applied, in order to reset and initialize the circuitry. Consequently, the device would resume WAIT state. As indicated, the Idle time is specified as the time interval following the initialization sequence until the last bit of the Command Sequence that is send to the transponder.

In case one of the Read Only modes is enabled, the device enters READ ONLY state, if the first two bits of the START_AUTH command are not being recognized within the time-out period $t_{WAIT,SA}$. In this case, Read Only operation commences $t_{WAIT,RO}$ after termination of the initialization sequence, t_{INIT} , see Figure 23. For details refer to section 7.5.

In order to force a LF Field Power-On Reset and proper device initialization at any time, the LF field OFF condition must be applied for at least $t_{RESET,SETUP}$, in order to ensure that the internal device supply voltage, V_{DD} , drops below the threshold voltage (V_{THR}), see Figure 24.

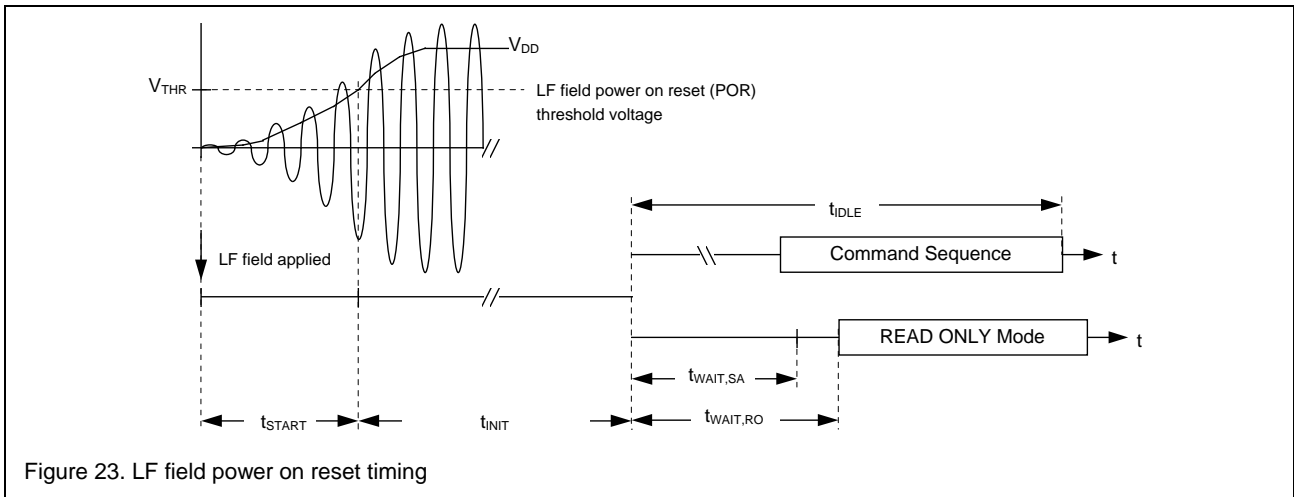


Figure 23. LF field power on reset timing

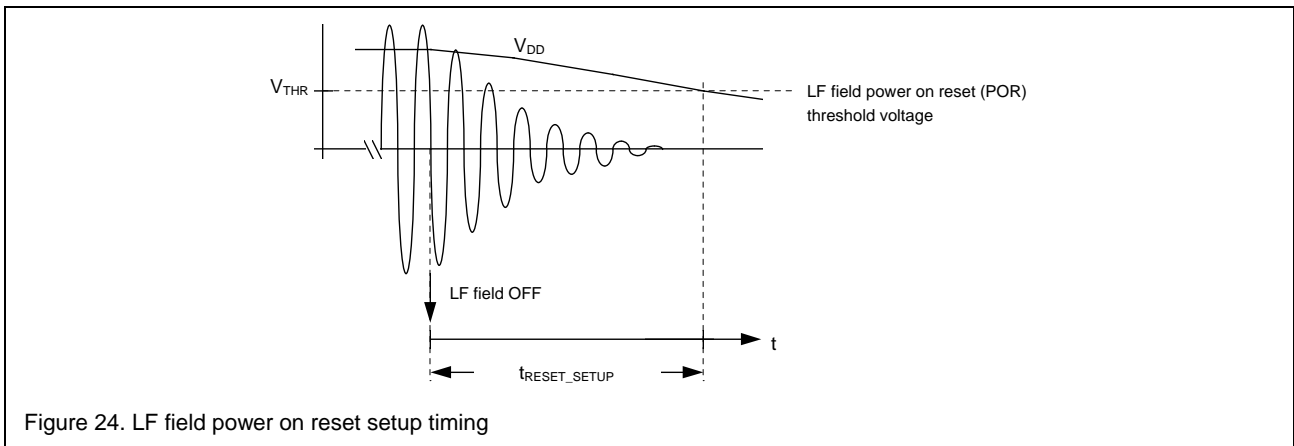


Figure 24. LF field power on reset setup timing

Security Transponder (HITAG2)

PCF7936AS

8 EEPROM CONTENT AT DELIVERY

The PCF7936AS EEPROM content is initialized during device manufacturing, according to Table 5.

However the EEPROM content may be modified as desired by the application, except for the page 0 block 0 which holds the Identifier (IDE) and serves the function of a serial number and product type ID.

Table 5. EEPROM Content Upon Delivery

bit 31	bit 0		
Content [HEX]		Page	Note
XX XX XX 1X		0	1
4D 49 4B 52		1	
XX XX XX XX		2	
06 AA 48 54		3	2
XX XX XX XX		4	
XX XX XX XX		5	
XX XX XX XX		6	
XX XX XX XX		7	

Note

1. Bit 7 to 4 of this page (Identifier) serve the function of a product type (application) identifier and are set to '0001' for the PCF7936AS.
2. Initially the device is configured for Password mode with the Transport Key (Password Basestation, PSW_B, as specified (page1)). The customer as desired for the application may change the configuration.
3. Locations marked 'X' are undefined and may hold any pattern.

Security Transponder (HITAG2)

PCF7936AS

9 LIMITING VALUES

All values are in accordance with Absolute Maximum Rating System (IEC 134)

PARAMETER	MIN	MAX	UNIT
Operating temperature range	-40	+85	°C
Storage temperature range	-55	+125	°C
Magnetic flux density (resistance against magnetic pulses)		0.2	T
Vibration - 10 - 2000Hz - 3.axis - IEC 68-2-6, Test Fc		10	g
Shock - 3.axis - IEC 68-2-27, Test Ea		1500	g
Mechanical stress (F_{MAX}), Note 1		10	N

Note

1. F_{MAX} is specified as indicated in Test Setup, section 11.

Security Transponder (HITAG2)

PCF7936AS

10 DEVICE CHARACTERISTICS

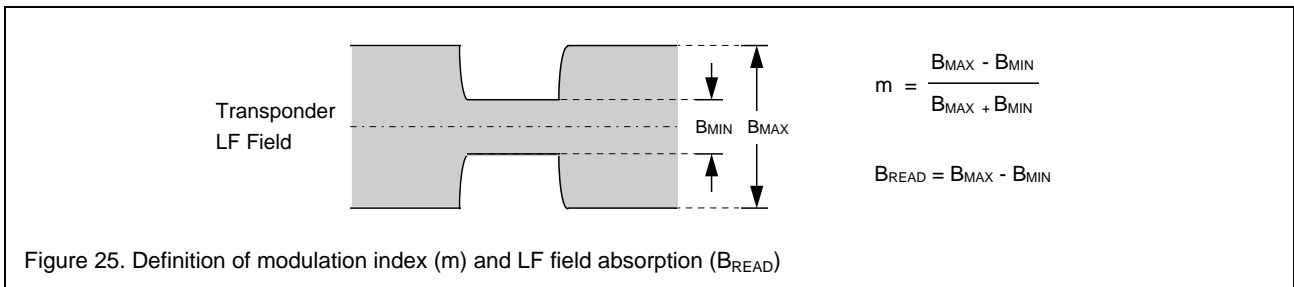
10.1 Electrical Characteristics

Tamb = -40 to +85°C, fSYS = 125kHz, TO = 1/fSYS. Unless otherwise specified

SYMBOL	PARAMETER	CONDITION	MIN	TYP	MAX	UNIT
Operating Conditions						
fRES	Resonance frequency		121		129	kHz
BW	Bandwidth		2.3			kHz
BTHR	Magnetic flux density, Read direction		35		400	μT _{PP}
BPRG	Magnetic flux density, Note 1 For EEPROM programming	m = 0,95, T _{WRP} = 8 T _O	35		400	μT _{PP}
B _{AUT}	Magnetic flux density, Note 1 For device authentication	m = 0,95, T _{WRP} = 8 T _O	35		400	μT _{PP}
B _{READ}	LF field absorption in read direction, Note 1	B _{FIELD} = 35 μT _{PP}	8			μT _{PP}
M _{PRG}	Minimum modulation index (m), Note 1 Write direction, device programming and authentication	B _{FIELD} = 35 μT _{PP} , T _{WRP} = 8 T _O			95	%
EEPROM						
T _{RET}	Data retention time	Tamb = 50°C	20			years
N _{WR-CYL}	Write endurance, page 1 to 7		100 k			cycle

Note

1. Modulation index (m) and LF Field absorption (B_{READ}) are defined according to Figure 25.
2. Parameters are measured with the Scemtech test equipment STM-1 in a Helmholtz arrangement according to section 11.



Security Transponder (HITAG2)

PCF7936AS

10.2 Timing Characteristics

$T_{amb} = -40$ to $+85^{\circ}\text{C}$, $f_{SYS} = 125\text{kHz}$, $T_O = 1/f_{SYS}$. Unless otherwise specified

SYMBOL	PARAMETER	CONDITION	MIN	TYP	MAX	UNIT
Command Handling						
$t_{WAIT,Tr}$	Transponder response delay		199		206	T_O
$t_{WAIT,Bs}$	Basestation response delay		90			T_O
t_{PROG}	EEPROM erase/write time			615		T_O
t_{IDLE}	Idle time				80	ms
Data Transmission						
T_{BIT}	Bit duration			32		T_O
T_{WRP}	Write pulse width	Note 1	4		10	T_O
$T_{LOG,0}$	Write pulse repetition time, logic 0		18		22	T_O
$T_{LOG,1}$	Write pulse repetition time, logic 1		26		32	T_O
T_{STOP}	Write pulse length, stop condition		36			T_O
LF Field Power On Reset, Note 2						
t_{START}	Transponder initialization time	$B_{FIELD} = 35\mu\text{T}$		80		μs
t_{INIT}	Transponder initialization time			225		T_O
$t_{RESET,SETUP}$	LF Field Power On Reset setup time	$B_{FIELD} = 100\mu\text{T}$	5			ms
Read Only Mode						
$t_{WAIT,SA}$	Timeout for START_AUTH command			320		T_O
$t_{WAIT,RO}$	Read Only Mode startup delay	Note 3		326		T_O

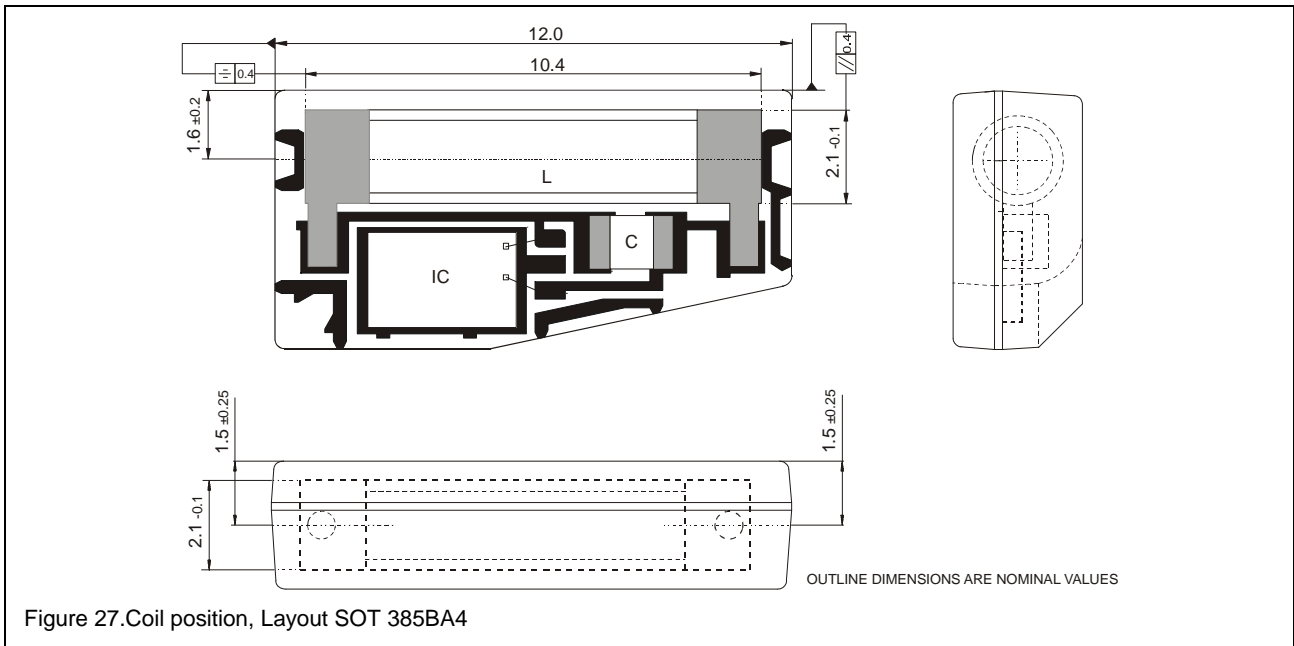
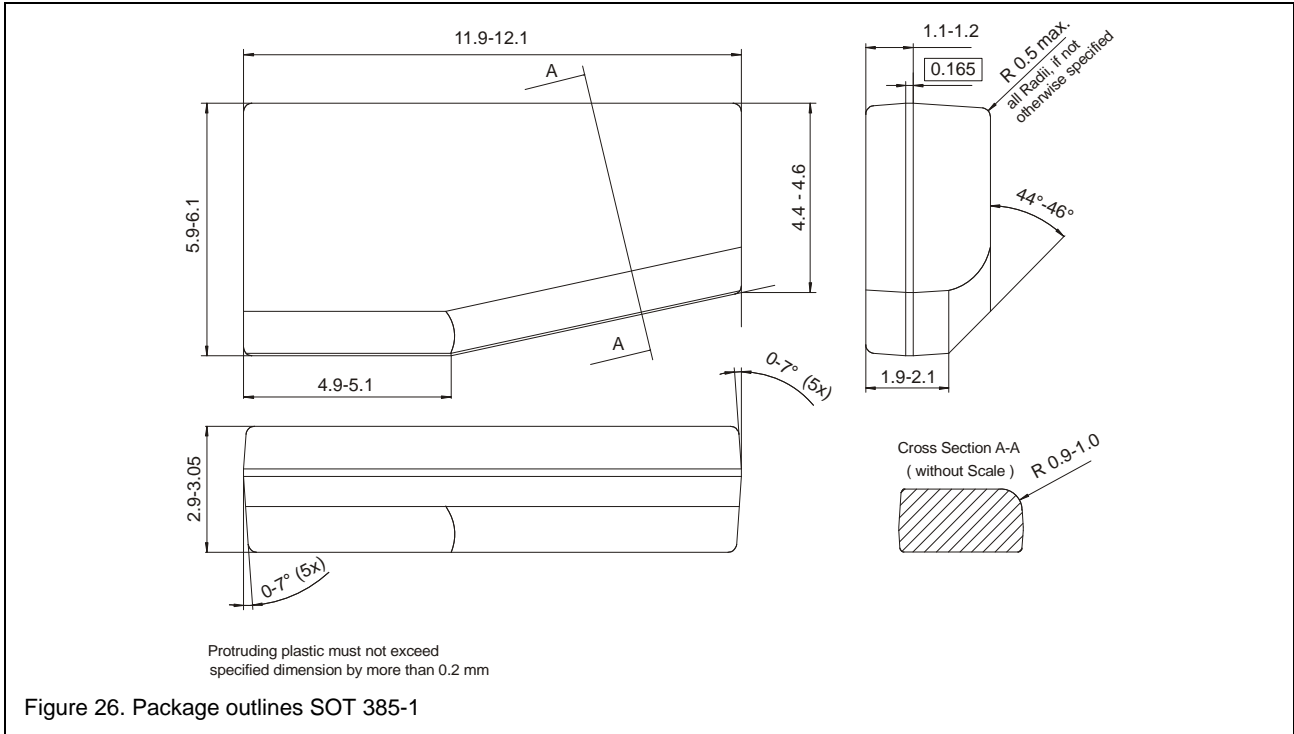
Notes

- As detected by the transponder interface demodulator. The corresponding LF Field write pulse width applied by the basestation depends on the resonance circuit properties and actual system coupling factor.
- Characterized with the Scemtech test equipment STM-1 in a Helmholtz arrangement according to section 11.
- Total delay ($T_{init} + T_{wait,RO}$) = 551 T_O

Security Transponder (HITAG2)

PCF7936AS

10.3 Mechanical Characteristics



Security Transponder (HITAG2)

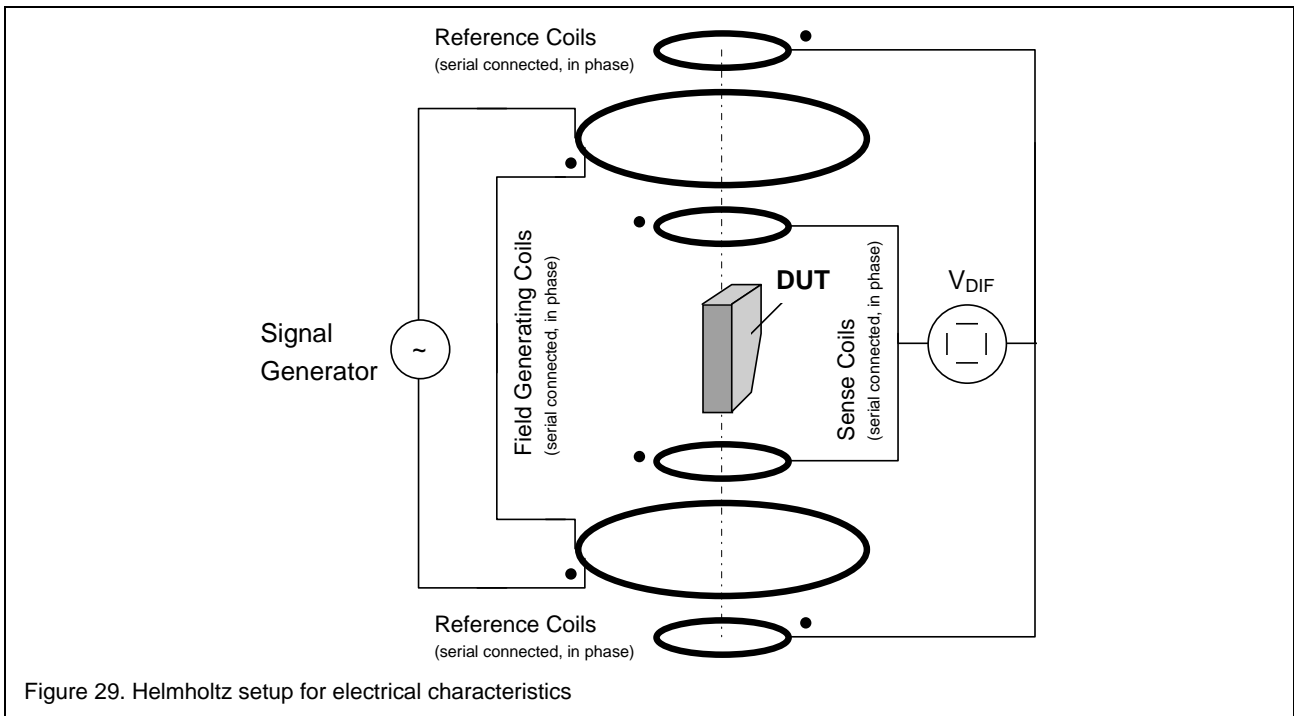
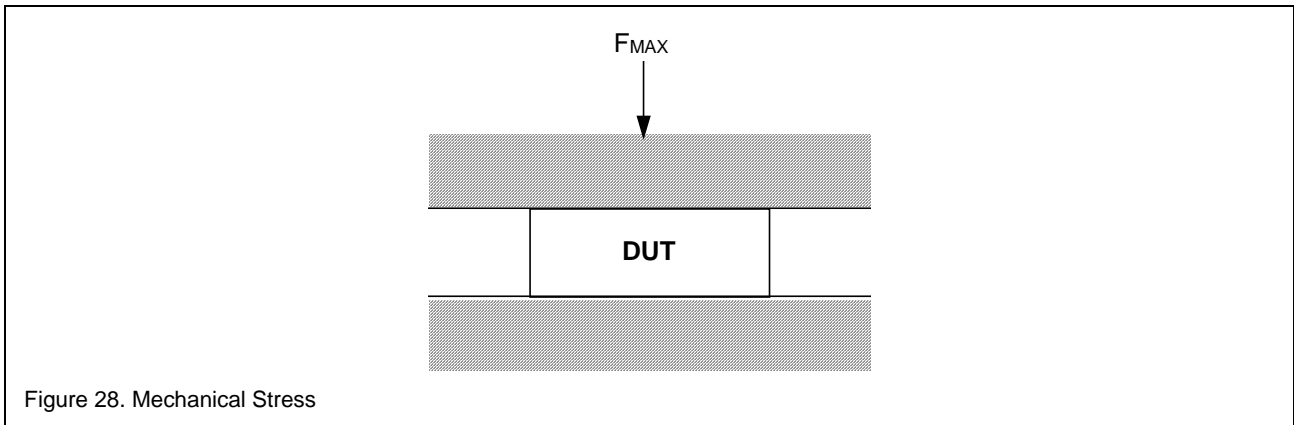
PCF7936AS

11 TEST SETUP

Device characteristics are measured according to the test setups given below.

Electrical characteristics are measured in a Helmholtz arrangement that generates an almost homogenous magnetic field at the position of the device under test (transponder), see Figure 29.

The sense coils detect the absorption modulation induced by the transponder, whereas the reference coils sense the magnetic flux generated by the field generating coils only. The voltage difference measured between the sense coils and reference coils is proportional to the magnetic field absorption induced by the transponder.



Security Transponder (HITAG2)

PCF7936AS

12 DEVELOPMENT TOOLS

Reference	Name	Description
OM6705	TED-Kit	Transponder Evaluation and Development Kit

13 REVISION HISTORY

Revision	Page	Description
2000 Apr 04	9, 10 14	Revised and updated revision PWP2 renamed PG3L and CSelect renamed DCS Specification of t_{IDLE} extended and updated
2003 May 15	7	Editorial changes and correction Changes regarding the Transponder Configuration become effective after a device reset or initialization sequence only.
2007 Nov 28	4	Change to NXP 'unique IDE' is replaced with 'quasi unique IDE'. IDE coderange is depleted and numbering is restarted (at 00h)
2007 Nov 30	28	Corrected Read Only Mode startup delay $t_{WAIT,RO}$ to $326 T_O$
2009 Feb 25	5	Fixed missing Figure 1. Block Diagram
2010 May 04	4	Added Type PCF 7936AS/3851/C with new manufacturing site ICN

Security Transponder (HITAG2)

PCF7936AS

14 LEGAL INFORMATION**14.1 Data sheet status**

Document status	Product status	Definition
Objective [short] data sheet	Development	This document contains data from the objective specification or 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

14.2 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.

14.3 Disclaimers**General**

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.

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 a 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.

Limiting values

Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) may cause permanent damage to the device. Limiting values are stress ratings only and operation of the device at these or any other conditions above those given in the Characteristics sections of this document is not implied. Exposure to limiting values for extended periods may affect device reliability.

Terms and conditions of 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>, including those pertaining to warranty, intellectual property rights infringement and limitation of liability, unless explicitly otherwise agreed to in writing by NXP Semiconductors. In case of any inconsistency or conflict between information in this document and such terms and conditions, the latter will prevail.

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.

Please be aware that important notices concerning this document and the product(s) described herein, have been included in the section 'Legal information'.



© NXP B.V. All rights reserved.

For more information, please visit: <http://www.nxp.com>
For sales office addresses, email to: sales.addresses@www.nxp.com