DATA SHEET

PCF7936AS

Security Transponder (HITAG2)

Product Specification (DRAFT) 2000 Mar 05

Confidential

Philips
Semiconductors

CONTENT

1 FEATURES

- Security Transponder for use in contactless authentication applications
- Data transmission and energy supply via LF link
- 32 bit 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 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 prove 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 filed.

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

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

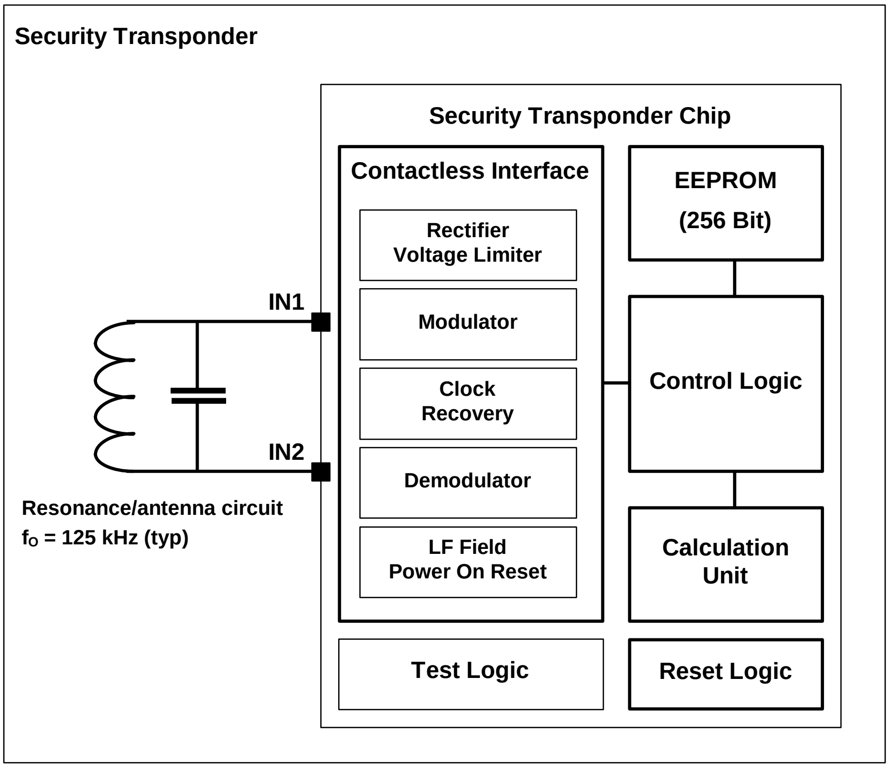


Figure 1. Block Diagram

5 TYPICAL APPLICATION

Figure 2. Typical Application

6 QUICK REFERENCE DATA

PARAMETER		VALUE	UNIT
Carrier frequency		125	kHz
Data rate - read - write		 4.0 5.2	 kbit/s kbit/s
Data coding - read - write		 Manchester or Bi-Phase Binary Pulse Length Modulation (BPLM)	
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	• Ciphered mutual authentication • Ciphered data transmission • 128 bit user EEPROM with programmable write protection • Read/Write Password mode • Read Only emulation modes (H400x, ISO 11784/85 and PCF7931)		

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.

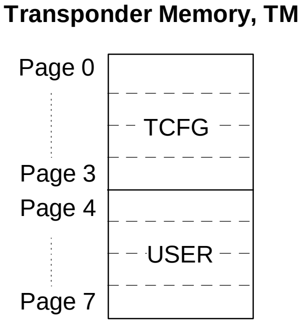


Figure 3. Memory Organization

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.

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.

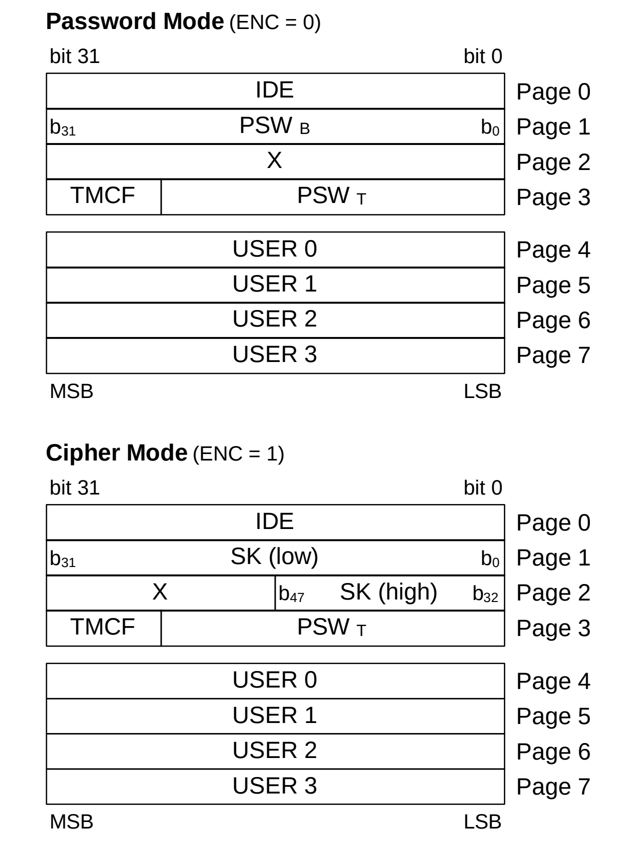


Figure 4. Transponder Memory Map

Note

1. 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.

Page 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 authorization method selected, page 1 and 2 do hold either 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 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 can not 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.

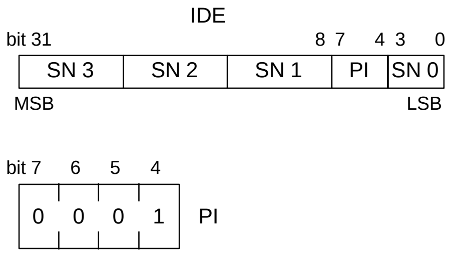


Figure 5. Identifier Organization, IDE

The Identifier, IDE, is incorporated in the process of device authentication and 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

Philips 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.

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.

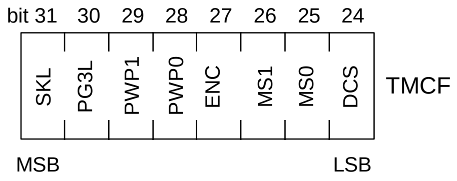


Figure 6. Transponder Memory Configuration, TMCF

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). Thus 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 can not 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 can not 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.

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	MIRO	1
0	1	ISO 11784/5	
1	0	PCF7931/30/35	2
1	1	Disabled	

Note

1. Features compatibility with H400x like Read Only transponders
2. Features compatibility with Philips' 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 cleared, 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.

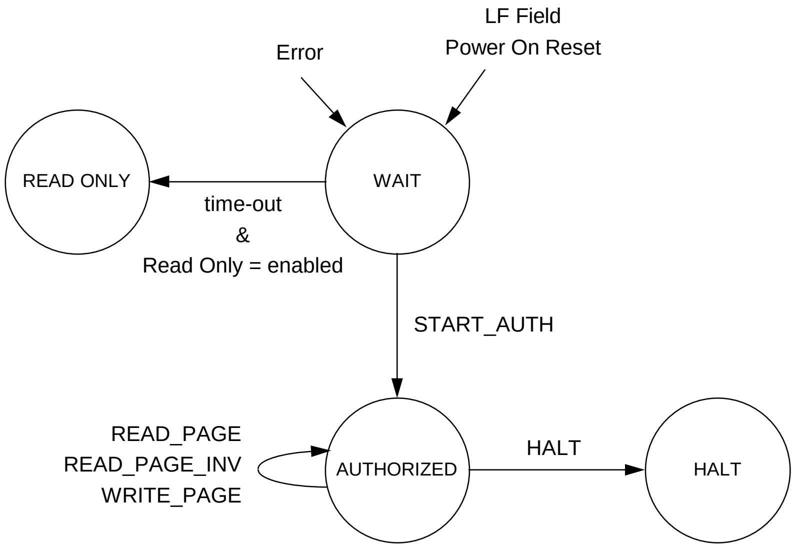


Figure 7. Transponder State Diagram

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, if no command is being issued before, for details refer to section 7.5.

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, upon which the device enters the WAIT state.

7.2.1 WAIT State

In wait state general memory accessed 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.

If the device enters WAIT state after a LF Field Power-On reset and one of the Read Only modes is enabled, the device will enter READ ONLY state after the specified time-out, if no START_AUTH command is being issued before. At least the first two command bits of START_AUTH need to be recognized by the device within the specified time-out period.

???? If the device enters WAIT state because of an error condition the READ ONLY state will not be entered at all.

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 ????

1. 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 a LF Field Power-On Reset condition and termination of the specified time-out, 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.

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

7.3.1 Command Description

The general form of a control sequence consist 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 consist 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 consist 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 to repeat 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.

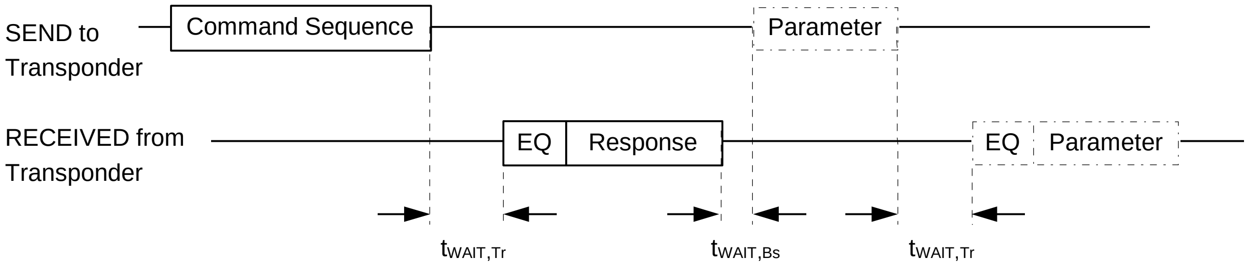


Figure 8. General control sequence timing

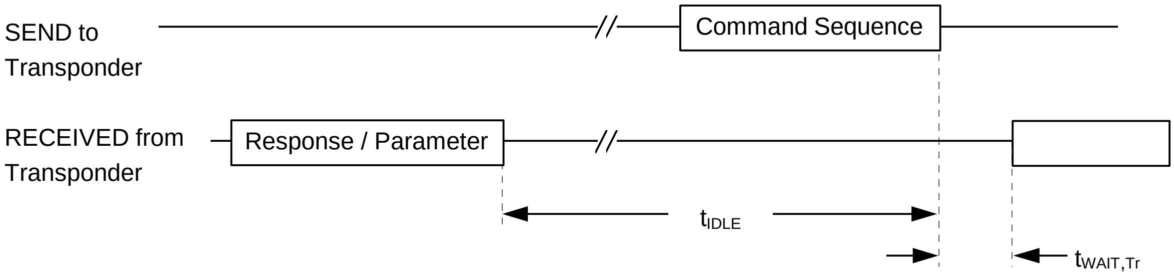


Figure 9. Command Idle Time

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 it will be accepted by the device, 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 it will be accepted by the device, see Figure 11. If accepted, the command Response consist 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.

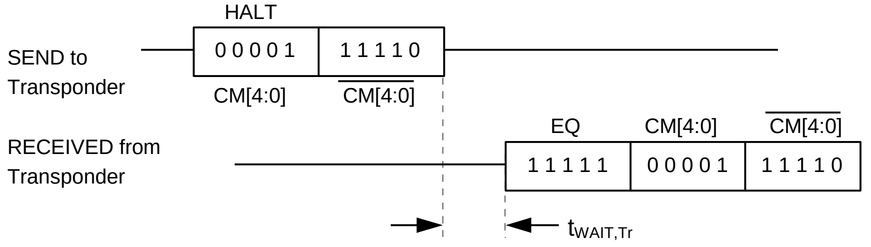


Figure 10. HALT timing

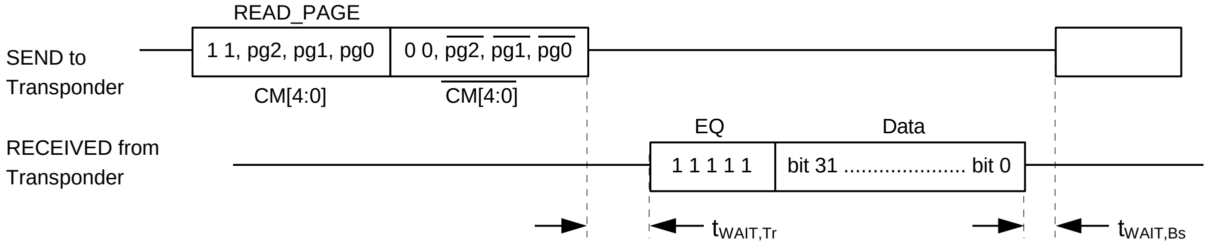

READ_PAGE
SEND to Transponder
1 1, pg2, pg1, pg0
0 0, $\overline{pg2}$, $\overline{pg1}$, $\overline{pg0}$
CM[4:0]
$\overline{CM[4:0]}$
RECEIVED from Transponder
EQ
Data
1 1 1 1 1
bit 31 .... bit 0
$t_{WAIT,Tr}$
$t_{WAIT,Bs}$

Figure 11. READ_PAGE timing

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 it will be accepted by the device, see Figure 12. If accepted, the command Response consist 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.

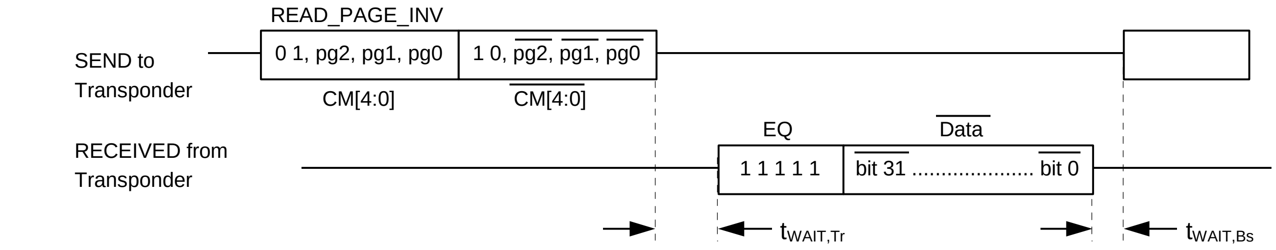

READ_PAGE_INV
SEND to Transponder
0 1, pg2, pg1, pg0
1 0, $\overline{pg2}$, $\overline{pg1}$, $\overline{pg0}$
CM[4:0]
$\overline{CM[4:0]}$
RECEIVED from Transponder
EQ
$\overline{Data}$
1 1 1 1 1
$\overline{bit\ 31}$ .... $\overline{bit\ 0}$
$t_{WAIT,Tr}$
$t_{WAIT,Bs}$

Figure 12. READ_PAGE_INV timing

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. No further Response will be send by the device 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.

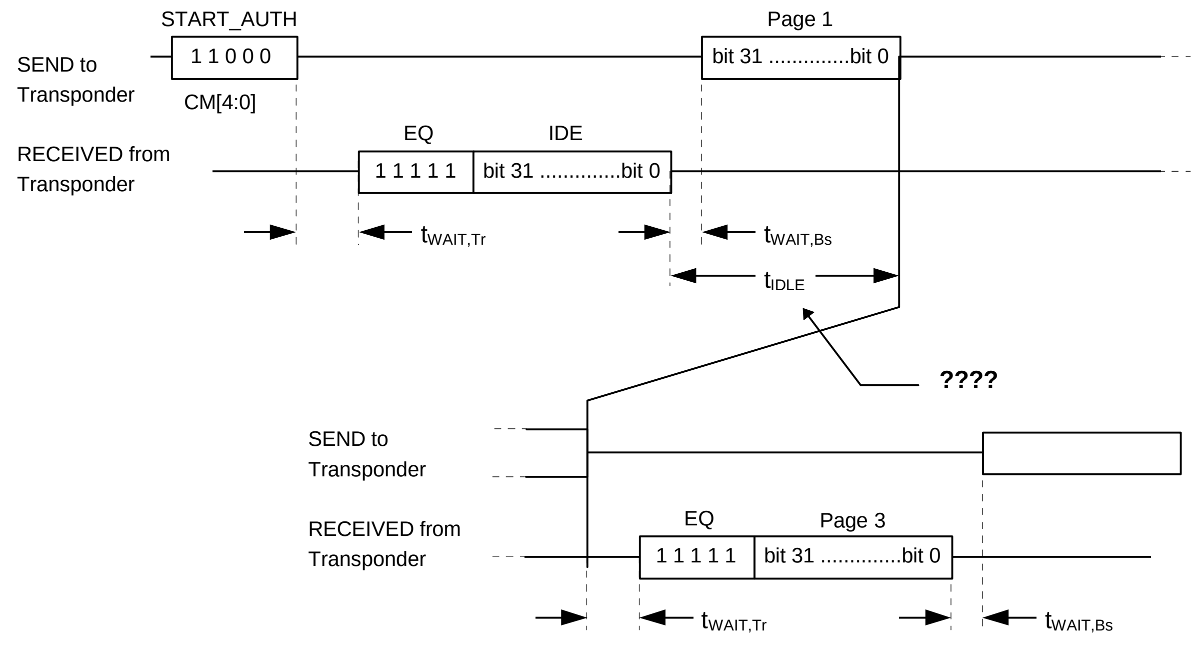


Figure 13. START_AUTH timing

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 consist of the ciphered content of page 3 block 0 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. No further Response will be send by the device 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 Philips representative for more information.

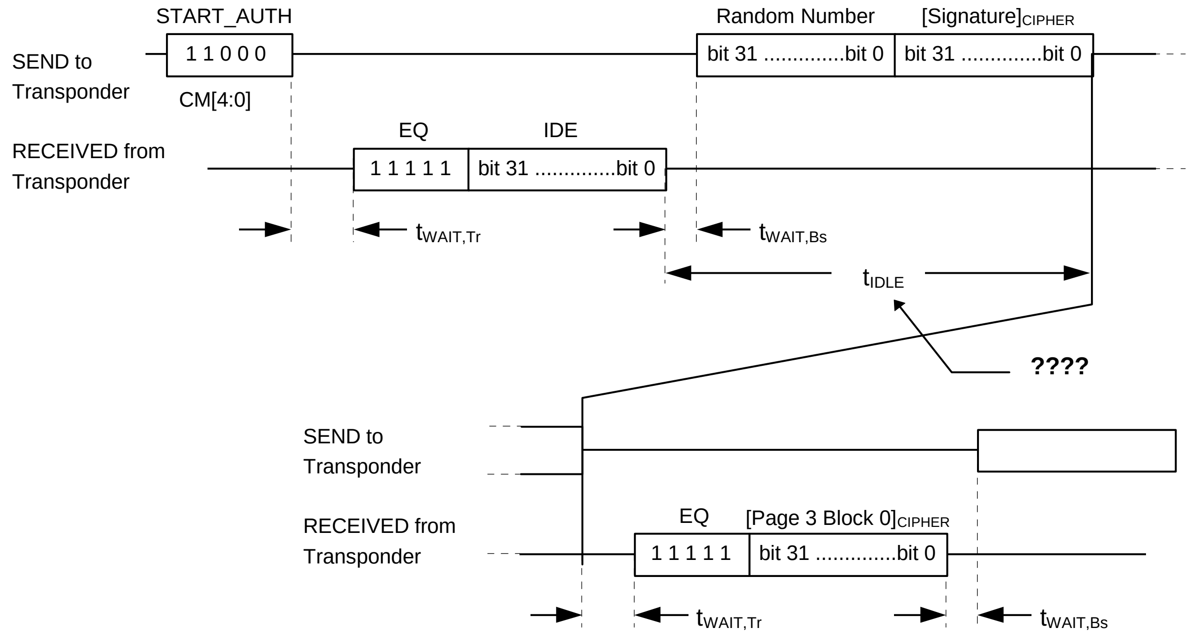


Figure 14. START_AUTH timing

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 it will be accepted by the device, 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.

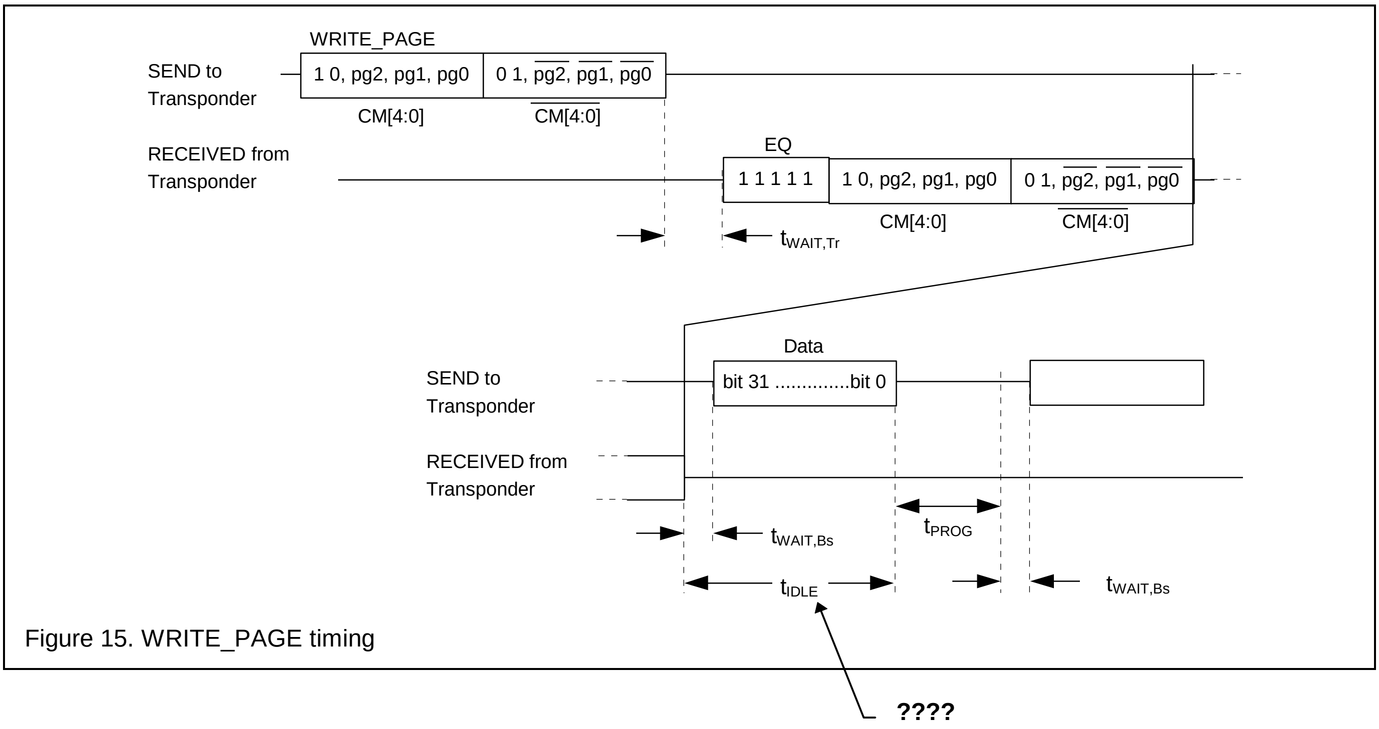


Figure 15. WRITE_PAGE timing

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 an 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 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 Philips representative for more information.

7.5 Read Only Modes

7.5.1 MIRO Mode

7.5.2 ISO 11784/5

7.5.3 PCF7931/30/35

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 16.

In read direction the device employs either Manchester or CDP encoding of data, see Figure 17, according to the setting of the Immobilizer Configuration bit DCS, which is part of the Transponder and Memory Configuration bits, TMCF, 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.

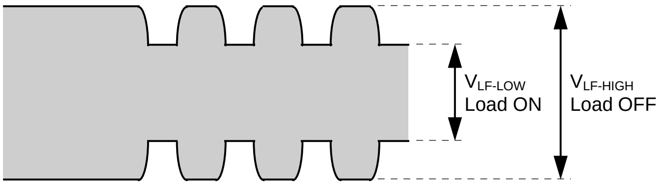


Figure 16. LF Field Absorption Modulation

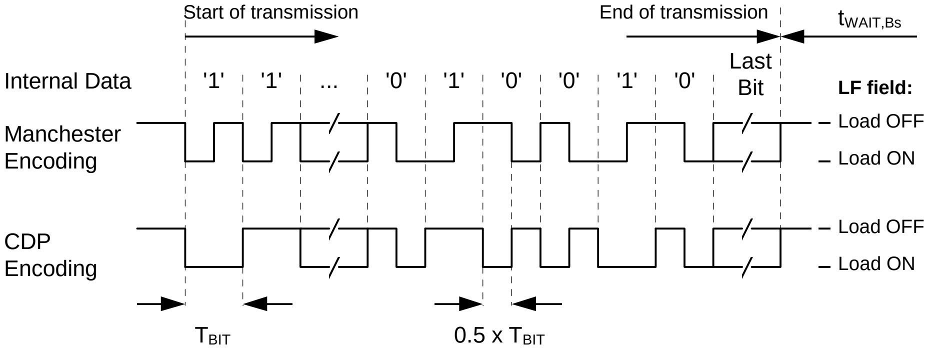


Figure 17. Data Transmission in Read Direction

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 are 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 18.

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 19.

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.

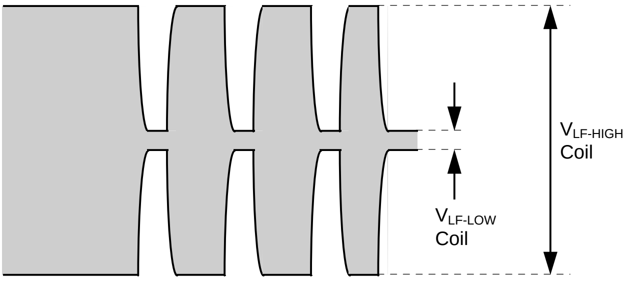


Figure 18. ASK Modulation of LF Field by the Basestation

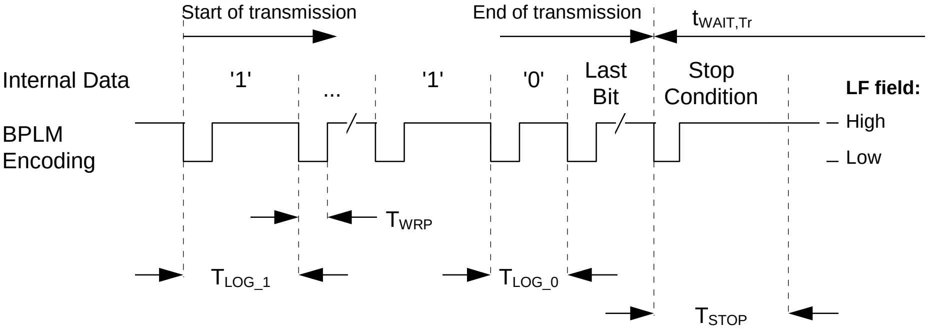


Figure 19. Data Transmission in Write Direction

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 20.

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 20. 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 20. 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 21.

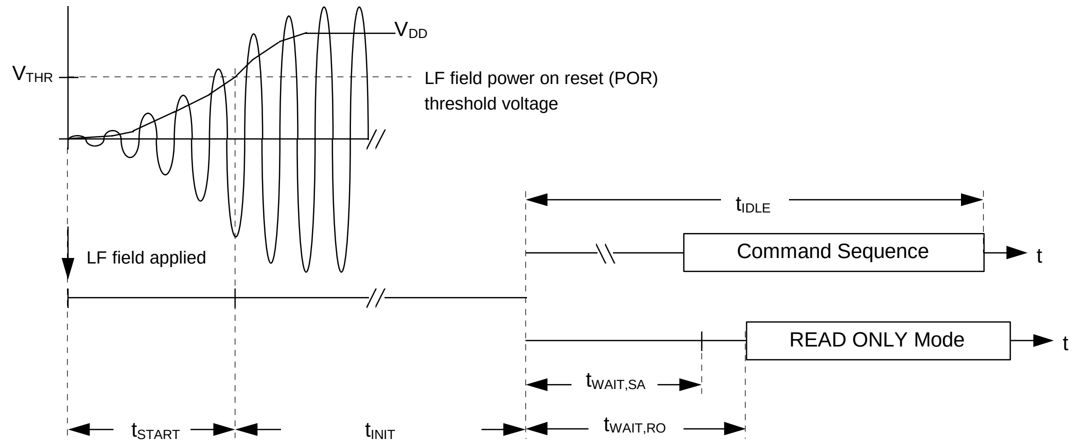


Figure 20. LF field power on reset timing

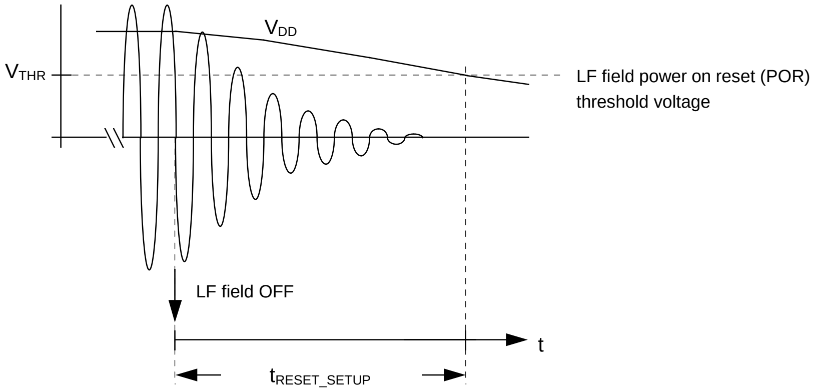


Figure 21. LF field power on reset setup timing

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 the 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 configuration may be changed by the customer as desired for the application.
3. Locations marked ‘X’ are undefined and may hold any pattern.

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.

10 DEVICE CHARACTERISTICS

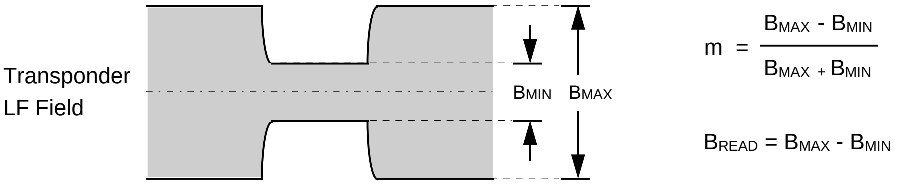
10.1 Electrical Characteristics

Tamb = -40 to +85°C, f_C = 125kHz, $T_O = 1/f_C$. Unless otherwise specified

SYMBOL	PARAMETER	CONDITION	MIN	TYP	MAX	UNIT
Operating Conditions						
f_O	Resonance frequency		121		129	kHz
BW	Bandwidth		2.3			kHz
B_{THR}	Magnetic flux density, Read direction		35		400	μT_{PP}
B_{PRG}	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	$B_{FIELD} = 35\ \mu T$, $T_{WRP} = 8\ T_O$	8			μT_{PP}
MI_{PRG}	Minimum modulation index (m), Note 1 Write direction, device programming and authentication	$B_{FIELD} = 35\ \mu T$, $T_{WRP} = 8\ T_O$			95	%
EEPROM						
T_{RET}	Data retention time	Tamb = 50°C	20			years
$N_{WR\text{-}CYL}$	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 22.
2. Parameters are measured with the Scemtech test equipment STM-1 in a Helmholtz arrangement according to section 11.



$$m = \frac{B_{MAX} - B_{MIN}}{B_{MAX} + B_{MIN}}$$

$$B_{READ} = B_{MAX} - B_{MIN}$$

Figure 22. Definition of modulation index (m) and LF Filed absorption (B_{READ})

10.2 Timing Characteristics

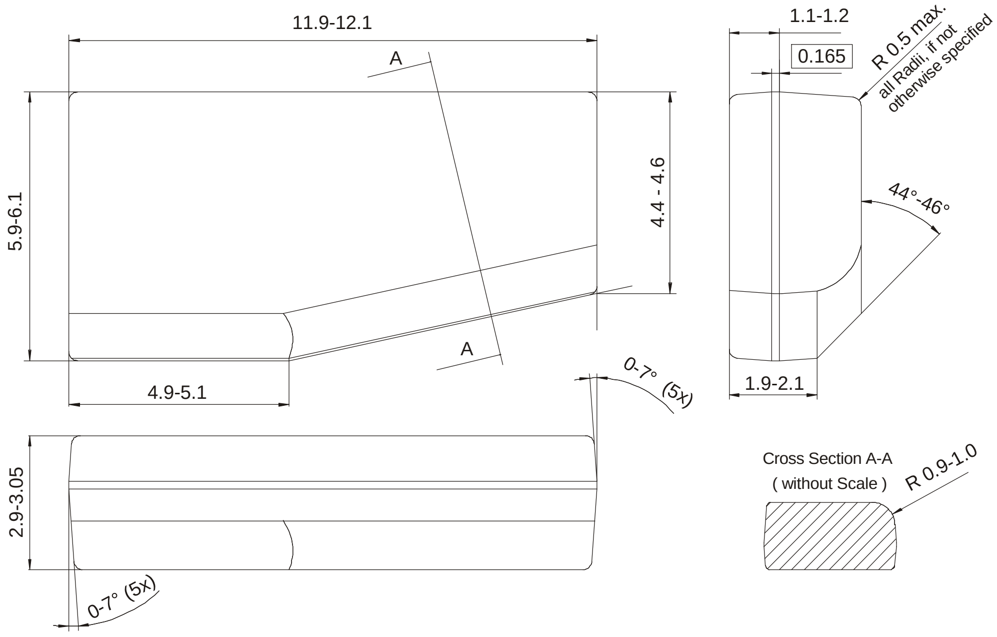
Tamb = -40 to +85°C, f_C = 125 kHz (typical), $T_O = 1/f_C$. Unless otherwise specified

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						
t_{START}	Transponder initialization time	B_{FIELD} = 35µT		80		µs
t_{INIT}	Transponder initialization time			225		T_O
$t_{RESET,SETUP}$	LF Field Power On Reset setup time	B_{FIELD} = 100µT	5			ms
Read Only Mode						
$t_{WAIT,SA}$	Timeout for START_AUTH command			320		T_O
$t_{WAIT,RO}$	Read Only Mode startup delay			551		T_O

Notes

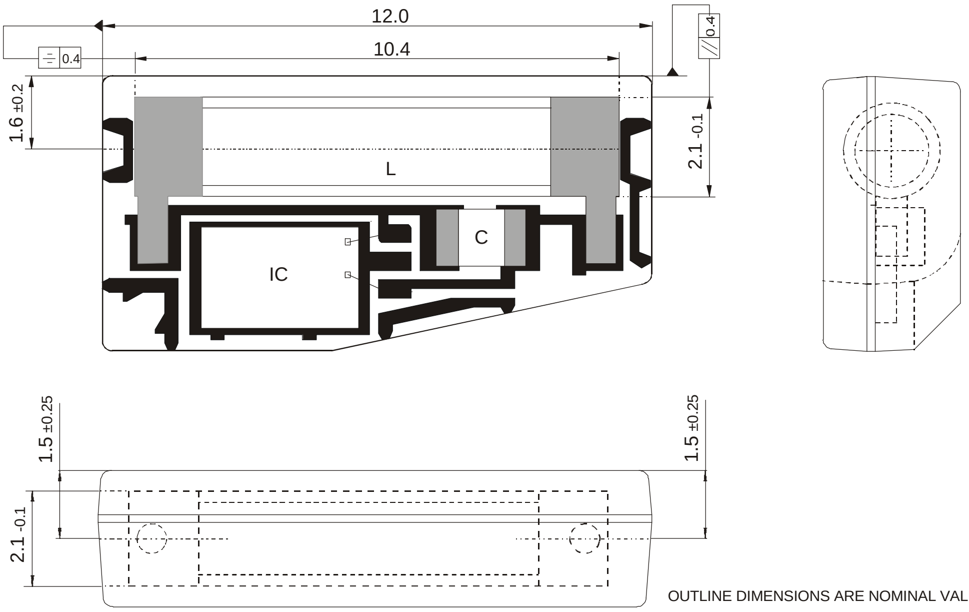
1. As detected by the transponder interface demodulator. The corresponding LF field write pulse width applied by the basestation depends on the resonance circuit properties and actual system coupling factor.

10.3 Mechanical Characteristics



Protruding plastic must not exceed specified dimension by more than 0.2 mm

Figure 23. Package outlines SOT 385-1



OUTLINE DIMENSIONS ARE NOMINAL VALUES

Figure 24.Coil position, Layout SOT 385BA4

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 26.

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.

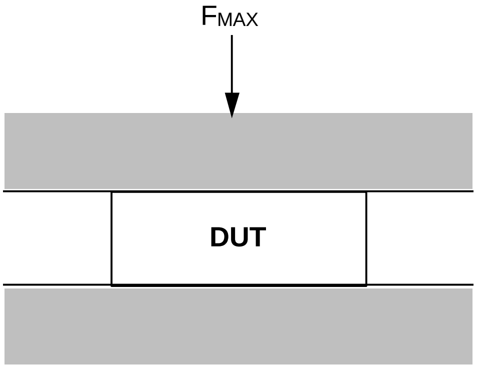


Figure 25. Mechanical Stress

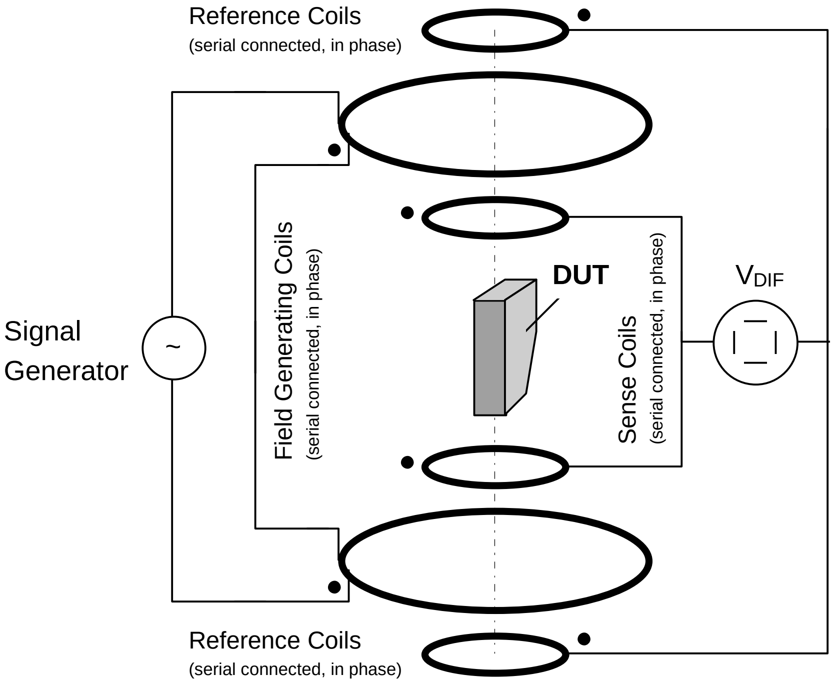

Reference Coils
(serial connected, in phase)
Signal
Generator
~
Field Generating Coils
(serial connected, in phase)
DUT
Sense Coils
(serial connected, in phase)
V_{DIF}
Reference Coils
(serial connected, in phase)

Figure 26. Helmholtz setup for electrical characteristics

12 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.	

13 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.

Philips Semiconductors - a worldwide company

Argentina: see South America
Australia: 34 Waterloo Road, NORTHRYDE, NSW 2113,
Tel. +612 9805 4455, Fax. +612 9805 4466
Austria: Computerstraße 6, A-1101 WIEN, P.O.Box 213,
Tel. +431 60 101, Fax. +431 30 101 1210
Belarus: Hotel Minsk Business Centre, Bld. 3, r.1211, Volodarski Str. 6,
220050 MINSK, Tel. +375172 200 733, Fax. +375172 200 773
Belgium: see The Netherlands
Brazil: see South America
Bulgaria: Philips Bulgaria Ltd., Energoproject, 15th floor,
51 James Bourchier Blvd., 1407 SOFIA
Tel. +3592 689 211, Fax. +3592 689 102
Canada: Philips Semiconductors/Components,
Tel. +1800 234 7381
China/Hong Kong: 501 Hong Kong Industrial Technology Centre,
72 Tat Chee Avenue, Kowloon Tong, HONG KONG,
Tel. +85223 19 7888, Fax. +85223 19 7700
Colombia: see South America
Czech Republic: see Austria
Denmark: Prags Boulevard 80, PB 1919, DK-2300 COPENHAGEN S,
Tel. +4532 88 2636, Fax. +4531 57 1949
Finland: Sinikalliontie 3, FIN-02630 ESPOO,
Tel. +3589 61 5800, Fax. +3589 61 580/xxx
France: 4 Rue du Port-aux-Vins, BP 317, 92156 SURESNES Cedex,
Tel. +331 40 99 6161, Fax. +331 40 99 6427
Germany: Hammerbrookstraße 69, D-20097 HAMBURG,
Tel. +4940 23 53 60, Fax. +4940 23 536 300
Greece: No. 15, 25th March Street, GR 17778 TAVROS/ATHENS,
Tel. +301 4894 339/239, Fax. +301 4814 240
Hungary: see Austria
India: Philips INDIA Ltd., Shivsagar Estate, A Block, Dr. Annie Besant Rd.
Worli, MUMBAI 400018, Tel. +9122 4938 541, Fax. +9122 4938 722
Indonesia: see Singapore
Ireland: Newstead, Clonskeagh, DUBLIN 14,
Tel. +3531 7640 000, Fax. +3531 7640 200
Israel: RAPAC Electronics, 7 Kehilat Saloniki St., TEL AVIV 61180,
Tel. +9723 645 0444, Fax. +9723 649 1007
Italy: Philips Semiconductors, Piazza IV Novembre 3,
20124 MILANO, Tel. +392 6752 2531, Fax. +392 6752 2557
Japan: Philips Bldg. 13-37, Kohnan 2-chome, Minato-ku, TOKYO 108,
Tel. +813 3740 5130,Fax. +813 3740 5077
Korea: Philips House, 260-199, Itaewon-dong, Yonsan-ku, SEOUL,
Tel. +822 709 1412, Fax. +822 709 1415
Malaysia: No. 76 Jalan Universiti, 46200 PETALING JAYA, Selangor,
Tel. +60 3750 5214, Fax. +603 757 4880
Mexico: 5900 Gateway East, Suite 200, EL PASO, Texas 79905,
Tel. +9 5800 234 7381
Middle East: see Italy
Netherlands: Postbus 90050, 5600 PB EINDHOVEN, Bldg. VB,
Tel. +3140 27 82785, Fax +3140 27 88399
New Zealand: 2 Wagener Place, C.P.O. Box 1041, AUCKLAND,
Tel. +649 849 4160, Fax. +649 849 7811
Norway: Box 1, Manglerud 0612, OSLO,
Tel. +4722 74 8000, Fax. +4722 74 8341
Philippines: Philips Semiconductors Philippines Inc.,
106 Valero St. Salcedo Village, P.O.Box 2108 MCC, MAKATI,
Metro MANILA, Tel. +632 816 6380, Fax. +632 817 3474
Poland: Ul. Lukiska 10, PL 04-123 WARSZWA,
Tel. +4822 612 2831, Fax. +4822 612 2327
Portugal: see Spain
Romania: see Italy
Russia: Philips Russia, Ul. Usatcheva 35A, 119048 MOSCOW,
Tel. +7095 247 9145, Fax. +7095 247 9144
Singapore: Lorong 1, Toa Payoh, SINGAPORE 1231,
Tel. +65350 2538, Fax. +65251 6500
Slovakia: see Austria
Slovenia: see Italy
South Africa: S.A. Philips Pty Ltd., 195-215 Main Road Martindale,
2092 JOHANNESBURG, P.O.Box 7430 Johannesburg 2000,
Tel. +2711 470 5911, Fax. +2711 470 5494
South America: Al. Vicente Pinzon, 173 - 6th floor,
04547-130 Sao Paulo, SAO PAULO - SP, Brazil,
Tel. +5511 821 2333, Fax. +5511 829 1849
Spain: Balmes 22, 08007 BARCELONA,
Tel. +343 301 6312, Fax. +343 301 4107
Sweden: Kottbygatan 7, Akalla, S-16485 STOCKHOLM,
Tel. +468 632 2000, Fax. +468 632 2745
Switzerland: Allmendstraße 140, CH-8027 ZÜRICH,
Tel. +411 488 2686, Fax. +411 481 7730
Taiwan: Philips Taiwan Ltd., 2330F, 66,
Chung Hsiao West Road, Sec. 1, P.O.Box 22978,
TAIPEI 100, Tel. +8862 382 4443, Fax. +8862 382 4444
Thailand: Philips Electronics (Thailand) Ltd.,
209/2 Sanpavuth-Bangna Road Prakanong, BANGKOK 10260,
Tel. +662 745 4090, Fax. +662 398 0793
Turkey: Talapasa Cad. No. 5, 80640 GÜLTEPE/ISTANBUL,
Tel. +90212 279 2770, Fax. +90212 282 6707
Ukraine: Philips Ukraine, 4 Patrice Lumumba Str., Building B, Floor 7,
252042 KIEV, Tel. +38044 264 2776, Fax. +38044 268 0461
United Kingdom: Philips Semiconductors Ltd., 276 Bath Road, Hayes,
MIDDLESEX UM3 5BX, Tel. +44181 730 5000, Fax. +44181 754 8421
United States: 811 Argues Avenue, SUNNYVALE, CA94088-3409,
Tel. +1800 234 7381
Uruguay: see South America
Vietnam: see Singapore
Yugoslavia: Philips, Trg N. Pasica 5/v, 11000 BEOGRAD,
Tel. +38111 625 344, Fax. +38111 635 777

For all other countries apply to: Philips Semiconductors, Marketing & Sales Communications,
Building BE-p, P.O.Box 218, 5600 MD EINDHOVEN, The Netherlands, Fax: +3140 27 24825

Internet: http://www.semiconductors.philips.com

SCB52

The information presented in this document does not form part of any quotation or contract, is believed to be accurate and reliable and may be changed without any notice. No liability will be accepted by the publisher for any consequence of its use. Publication thereof does not convey nor imply any license under patent- or other industrial or intellectual property rights.

**Philips
Semiconductors**

PHILIPS

Change Record

2000 Mar 05	First DRAFT release - PWP2 renamed PG3L - Cselect renamed DCS