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.

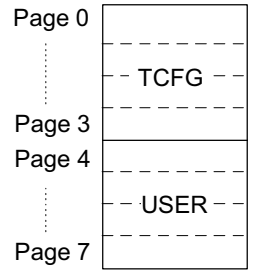

Figure 3. Memory Organization

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.

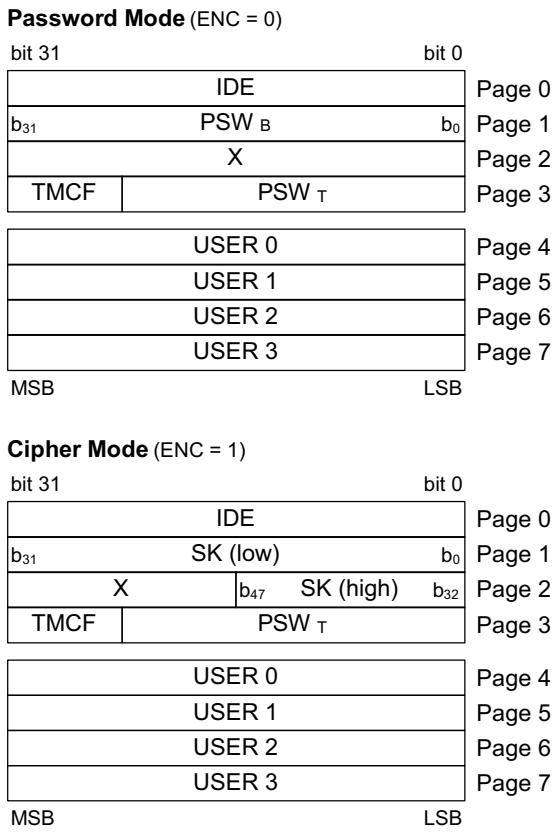

Figure 4. Transponder Memory Map

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.

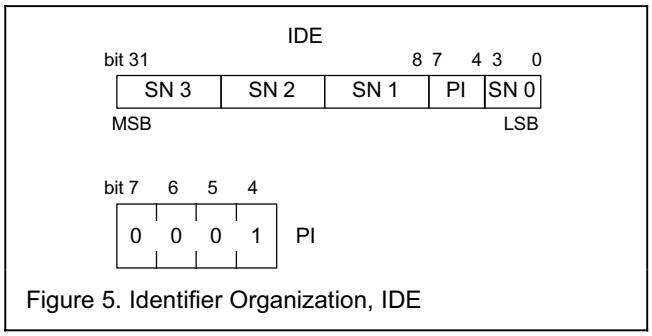

Figure 5. Identifier Organization, IDE

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.

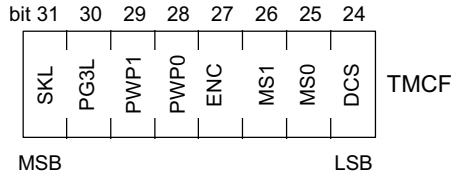

Figure 6. Transponder Memory Configuration, TMCF

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.