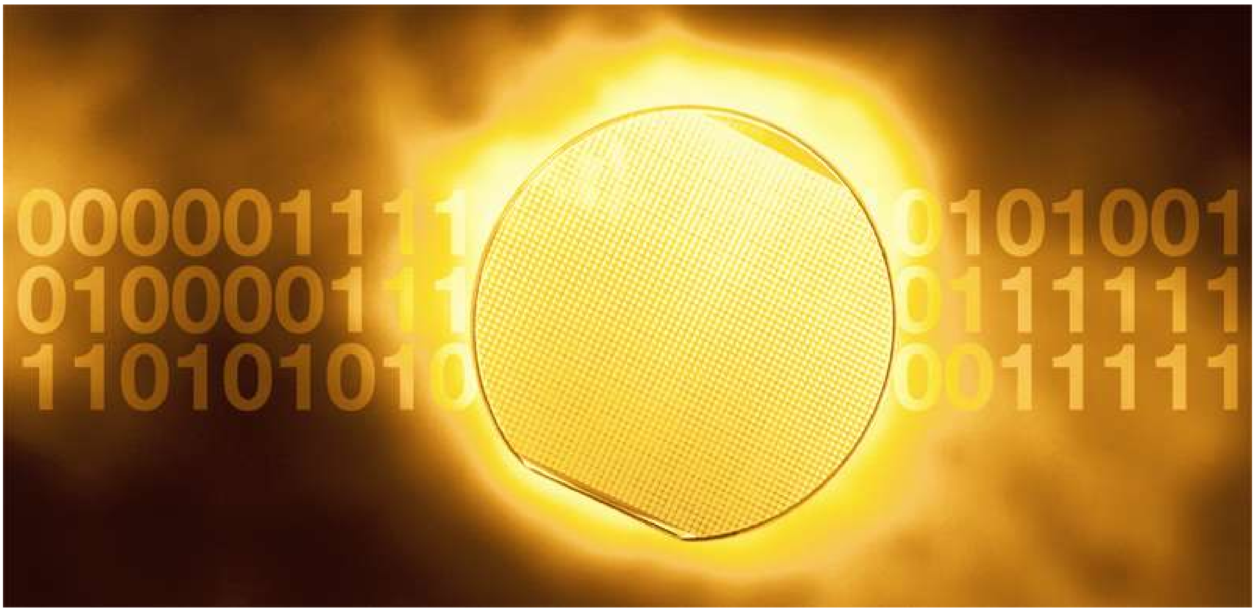
Inside CONTACTLESS

DATASHEET PICOPASS 2 KS



Chips > Packaging > Readers > more…

Version 1.0 : 30-11-2004

Published by:

INSIDE Contactless

11A, Parc Club du Golf

13856 Aix-en-Provence Cedex 3

France.

Tel.: +33 (0)4 42 39 63 00 - Fax: +33 (0)4 42 39 63 19

E-mail: info@insidefr.com - Web site: http://www.insidefr.com

INSIDE Contactless reserves the right to make changes, without notice, to any product herein to improve reliability, functionality, or design. INSIDE Contactless advises its customers to obtain the latest version of device data sheets to verify, before placing orders, that the information being relied upon by the customer is current.

Information furnished by INSIDE Contactless is believed to be accurate and reliable. However, INSIDE Contactless does not assume any liability resulting from the application or use of any product described within.

INSIDE Contactless‘ products are not authorized for use as critical components in life support devices or systems unless a specific written agreement pertaining to such intended use is executed between the manufacturer and INSIDE Contactless board.

Life support devices or systems are devices or systems that (a) are intended for surgical implant to the body or (b) support or sustain life, and whose failure to perform, when properly used in accordance with instructions for use provided in the labeling, can be reasonably expected to result in a significant injury to the user.

A critical component is any component of a life support device or system whose failure to perform can be reasonably expected to cause the failure of the life support device or system, or to affect its safety or effectiveness.

TABLE DES MATIÈRES

MAIN FEATURES

MEMORY

- 1 page 2K
    - page may be separated in two application areas protected by different keys
- EEPROM read/write memory organized by 8-byte block.
- Up to 7 independent blocks lockable by user fuses.
- Power-Guard® system **(anti-tearing)** for secure EEPROM writing.

CONTACTLESS COMMUNICATION

- Carrier frequency: **13.56 MHz ±7 KHz**.
- Data rate : 26 kBit/s (ISO 15 693), 106 or 424 KBit/s (ISO 14 443 type B)
- Data coding : User can configure :
    - ISO15693-2 (Fast Mode) & ISO 14443 B compliant with protocol auto-detection
- Fast anti-collision :
    - Up to 50 chips/s using protocol ISO15 693, and >100 chips using protocol ISO 14 443
    - Several chips can operate independently in the field.

DEDICATED LOGISTICS FEATURES

- Fast moving tags detection
- Batch processing

SECURITY FEATURES

- High security authentication (Secure pages only) :
    - Authentication using INSIDE Contactless' proprietary cryptographic algorithm.
    - 64-bit secret key, 32-bit challenge, 32-bit response.
    - One Debit Key (Kd) and one Credit Key (Kc).
        - Read and Write security :
    - Option 1 : 2 applications area protected by one key for each operation
    - Option 2 : Read protected by Kd, and Read/Write protected by Kc

    - Write protection by authentication and cryptographic signature.
- Secure e-purse (Secured pages only) :
    - 65534 units
    - up to 65535 recharges
    - Anti-tearing protection
    - Separate Increase and Decrease access protections
- Smart Electronic Article Surveillance (E.A.S.)
- Anti- tampering system

CHIP CARACTERISTICS

- EEPROM updating (erase and program) time: 5 ms per 8-byte block.
- EEPROM lifetime: >100 000 write/erase cycles.
- Data retention: minimum 10 years @85°C.
- Chip operating temperature range: from -40°C to +85°C.
    - Power consumption independent of data read in memory.
    - Internal personalization fuses.

HARDWARE SECURITY

- Unique **64-bit** chip serial number.
- Decrement-only feature for the **e-purse**
- Power consumption independent of data read in memory
- Anti-tearing design for the **e-purse**
    - Possibility to authorize authentication only in 14 443 type B protocol using Hardware protection.

Product Ordering Codes

Product	*Ordering code*	*Note*	*Package*	*Tools*
PicoPass 2KS	WF158H2KS-C35	Standard Low capacitance chip : 34 pF	Die, Module	Evaluation and Integration kits.
PicoPass 2KS	WF158H2KS-C97	High capacitance chip :94 pF	Die, Module	Couplers and Antennas. Libraries and Application Notes

Note : PicoPass is also available in contactless card, inlet, tag, coin tag, key fob or specific designed packaging. Please, contact us for further details.

1 CHIP BLOCK DIAGRAM

The chip is made up of 32 blocks of 64 bits of EEPROM memory, a digital logic part for controlling access to the memory and an analog interface for data and energy transmission.

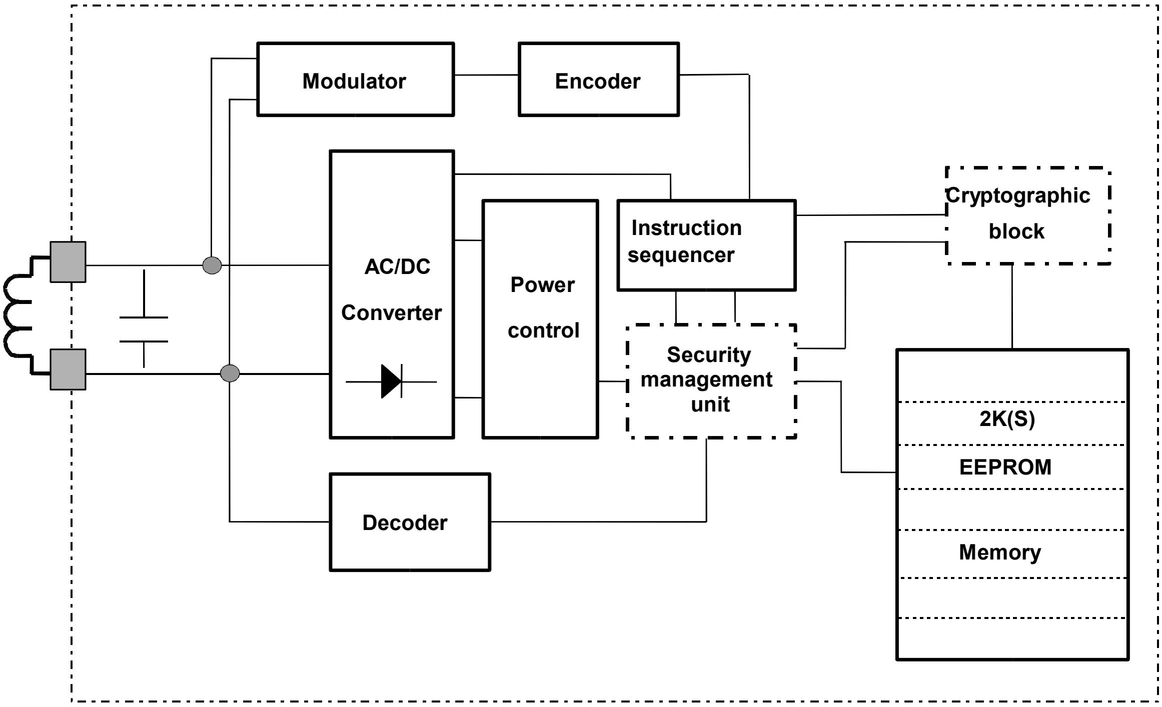


Fig. 1 CHIP BLOCK DIAGRAM

2 MEMORY MAPPINGS

2.1 Page mapping

Block	Size : 8 bytes
0	Serial Number (64 bits)
1	Configuration block
2	e-purse
3	Debit Key
4	Credit Key
5	Application Issuer Area
6	Application Area 1 : protected by kd
7	
8	
9	
10	
11	
12	***Modifiable limit***
13	
14	
-	Application Area 2 : protected by kc
31 (2K) or 255 (16K)	

Block 6 to 12 are write lockable

Fig. 2a MAPPING FOR 2KS or 16KS PAGE

Block	Size : 8 bytes
0	Serial Number (64 bits)
1	Configuration block
2	Application Issuer Area
3	Application Area
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
-	
31 (2K) or 255 (16K)	

Block 6 to 12 are write lockable

Fig. 3b MAPPING FOR 2K or 16K PAGE

2.2 MEMORY DESCRIPTION

This chapter contains the chip memory description. Features (like EAS, e-purse or anti-tampering feature) will be detailed in the next chapters.

2.2.1 SERIAL NUMBER

This area stores the unique 64-bit chip serial number which is set up during the production phase.
It is used in the anti-collision procedure.
Please, refer to chapter ANTICOLLISION PROCEDURE for further details.

2.2.2 Configuration block

This area is used to set all the chip options.

Block 1 features (for all pages)

Byte 0	Byte 1 & 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7
Appli Limit	Application 16-bit OTP Area	Block Write Lock	Chip Config.	Memory Config.	E.A.S	**Fuses**

This block enables to configure the chip:

- Security option (each page may be secured or unsecured depending on user's needs)
- Application limit for secured page
- Read and Write access

Chip configuration is protected by a fuse (Fuses byte). While this fuse is valid, user is allowed to modify this configuration. Chip is said in ***Personalization mode***. Once this fuse is blown, no configuration modification is allowed, and chip is ready to be use in the user application: chip is said in ***Application mode***.

Block 1 in Page 0: other features

- **RFU**

- **EAS**: A byte enables to set the Electronic Article Surveillance active or inactive. This feature enables fast chip detection. For more information, please see chapter **E.A.S.**

The **EAS**, **Memory Config.** and **Chip Config.** bytes are global for the chip (only active in page 0 block 1). These 3 Bytes are RFU for the pages 1 to 7 in multi application configuration.

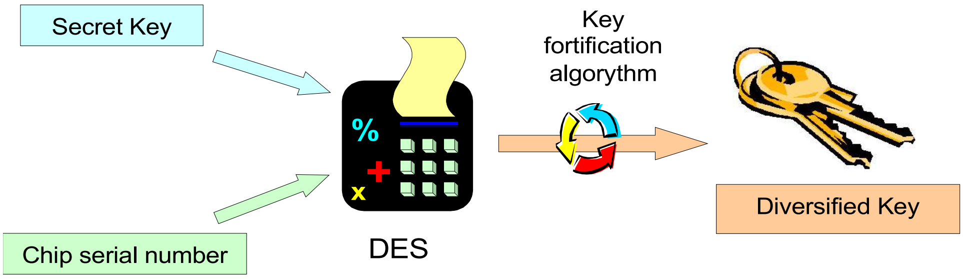
Important note: Access to this area is limited. See the next chapter for all access information.

2.2.3 Secret Keys & keys diversification

These blocks (2 x 8 bytes) contains chip secret keys. It is not possible to read these values.
Keys can be written while the chip is in *personalization mode* (i.e. while fuses are not blown and chip configuration can be changed). However, 2 bits in the configuration block (byte 7: fuses) enable the user to keep to possibility to modify the keys when the chip is in *Application mode* (i.e. fuses are blown, security options and memory configuration cannot be modified anymore).

In the chip is written the result of the diversification of the key value and the serial number. This increase the chip security as, even if 2 chips are configured with the same application key (Kd and Kc), they will have in their memory different value.

The diversification principle is described in the following diagram:



For all the security operation (authentication, signature calculation), coupler first have to calculate the diversified key (coupler must know the key, selected chip returns its serial number). Then it is able to authenticate and write data in the secured chip.

2.2.4 Electronic purse (Secured chips only)

This block is used as a 65534-unit value area reloadable 65535 times.
Increment of this value area is secured by Credit Key and decrement is secured by Debit Key. Thus a user may be allowed only to decrement the **e-purse** value, whereas another person may be allowed to credit it.
It can also be used as a “decrease only” counter on 32 bits if user needs more than 65534 units.
Please, refer to chapter **e-purse** for further details.

2.2.5 APPLICATION ISSUER AREA

This area is made up of 1 block. Data that is stored in the Application Issuer Area becomes read only after chip is set in *application mode*.

It can be used, for instance, to recognize and separate different applications with the final customer name or identifier.

2.2.6 APPLICATION AREA

Description

It enables the user to read and write 26 blocks of 8 bytes in secured mode and 29 in non secured mode.

In the chip secured version, this area can be split in two independent parts with restricted access.

The limit position between the 2 application areas is can be set in the configuration block. Thus user can organize its memory so it fits to his needs.

Access condition

The Application area can be Read and Write for the application according to the rules, described below:

Chip	*Size (blocks)*	*R/W*	*Authentication with*
2KS	26	Secured	Debit Key for Application 1 Credit Key for Application 2
2K	29	Yes	No authentication needed

The application area can be cut in two distinct parts in the secured chip. Access to the first part of the memory is protected by the debit key. User has to perform an authentication based on the debit key to be able to read or write data in this area.
Access to the second part of the memory request an authentication with the Credit key.

When reading is not allowed, the chip answers FFh.
When writing is not allowed or if the address sent in the command is higher than the physical address memory, the chip does not answer and a new command can only be sent after 400 µs.

Block write lock

Blocks from 6 to 12 may be write locked. This is controlled by a bit in the configuration block (byte 4). Thanks to this byte it is also possible to write lock the entire chip. Thus it is only possible to read it, but **e-purse** will not work anymore

3 Chip configuration and personnalization flow

Chip configuration is defined in the Configuration block (block 1).
Modify this block enable the user to set:

- Security option (each page may be secured or unsecured depending on user's needs)
- Application limit for secured page
- Read and Write access

The first part of this chapter describes the chip configuration block.
The second part presents the various combination of memory mapping.
The third part introduces the chip personalization (keys).

3.1 Configuration block

This Area, located in Block 1 Page 0, is used to set all the chip options.

Block1	**Appli Limit**	**Application 16-bit OTP Area**	**Block Write Lock**	**Chip config.**	**Memory Config**	**E.A.S**	**Fuses**
	Byte 0	Byte 1 & 2	Byte 3	Byte 4	Byte5	Byte 6	Byte 7

The **EAS**, **Memory Config** and **Chip config** Bytes are global for the chip (only active in page 0 block 1) .
These 3 Bytes are RFU for the pages 1 to 7 in multi application configuration.

Important note: access to this block is limited: some bit may only be read, others may be written (1->0), and others may be erased (0 -> 1). The following tables show access rights for each bit. Be careful when writing in this area.

	Byte number of the page 0 / block 1							
Byte	***0***	***1***	***2***	***3***	***4***	***5***	***6***	***7***
Fpers	**Applications Limit**	**Application 16-bit OTP Area**		**Block Write Lock**	**Config**	**Memory config**	**E.A.S**	**Fuses**
1	r/w	r/w		r/w	r/w	r/w	r/w/e	*
0	r	r/w		r/w	r	r	r/w/e	*

	Byte 7 / Block 1 / page 0							
Bit	***7***	***6***	***5***	***4***	***3***	***2***	***1***	***0***
Fpers	Fpers	Coding1	Coding0	Crypt1	Crypt0	Fprod1	Fprod0	RA
1	r/w	r/w	r/w	r/w	r/w	r/w	r/w	r/w
0	r	r	r	r/w	r/w	r	r	r

r/w/e : read / write (OTP Area) / erase (EEPROM Area) allowed

3.1.1 FUSES

Bit	7	6	5	4	3	2	1	0
Designation	Fpers	Coding1	Coding0	Crypt1	Crypt0	Fprod1	Fprod0	RA

Fig. 4 Fuses mapping

Fpers :

When the page is in personalization mode this bit is equal to 1.
Once the application issuer has personalized and coded its dedicated areas, this bit must be set to 0: the page is "**in application mode**".

> *Note:*
>
> *Once the chip is in application mode, it is impossible to get the chip in personalization mode again.*
>
> *This bit **Fpers** is related to the selected page.*

Coding1 & Coding 0 :

These bits are used to choose the data coding versus ISO protocols.

Coding1	*Coding0*	*Input Data Coding*
1	1	RFU
1	0	RFU
0	1	ISO 14 443-2 Type B / ISO 15693
0	0	ISO 14 443 type B only

> *Notes :*
>
> *These bits **Coding 1 & 0** are related to the selected page. This means that user may have a data coding according to the selected page.*

Crypt 1 & Crypt 0 :

These bits are used to choose the cryptographic selection.

Crypt1	*Crypt0*	*Cryptographic selection*
1	1	Secured page Keys may be modified by user

Secured product

1	0	Secured page Keys values are locked
0	0	No authentication possible. Chip can be read only if bit RA (Read Access) is enabled.

Unsecured product

0	1	Non secured page

<u>Notes :</u>

*These bits **Crypt 0 & 1** are related to the selected page. This means that user can have a cryptographic mode according to the selected page.*

Once F1 is blown, it is not possible to change from a secured product (page) to an unsecured product (page).

To prevent the chip from locking, it is not possible to write CRYPT0 of a non secure page when Fpers is blown.

Fprod1 & Fprod0

These bits are used by Inside Contactless during manufacture. Their values are the following:
- Fprod1 = 1
- Fprod0 = 0

RA: (Read Access mode)

When this bit is set to 1 reading is always allowed. When it is set to 0 reading is allowed only after authentication.

If **Crypt 0** = **Crypt1** = 0 and **RA**=1, the whole chip memory is **Read Only**
If **Crypt 0** = **Crypt1** = 0 and **RA**=0, it is not possible to **Read** or **Write** any block in the chip memory except reading blocks 0 & 1.

*<u>Note:</u> This bit **RA** is related to the selected page. This means that user can have different Read Access modes according to the selected page.*

3.1.2 E.A.S

This byte is used for Electronic Article Surveillance and is located in Block 1 / page 0.
If MSB (most significant bit) of is set to 0, the chip will answer its serial number to the DETECT command. This enables fast chip detection.
If MSB is set to 1, chip do not respond, and go back to IDLE mode
Please, refer to chapter SMART E.A.S for further details.

3.1.3 Memory configuration

This byte is used to:

- Choose a key access configuration.
- Enable/disable authentication for 15693 protocol (long range protocol) for security reasons
- Enable 14443-3 protocol.
- Choose 1 or 2 books.

Memory length byte description is shown below.

bit7 16K	bit6 RFU	bit5 Book	bit4 2K	bit3 RFU	bit2 isoB-3	bit1 Lock Auth	bit0 Key Access

Key Access (book 0-1, page 0-7, block1, byte 5, bit 0)

Active low

This bit allows changing the key access conditions. When set to 1 the Area determine the Key to use, when set to 0 it's the operation (read or write)

	Authentication condition	
Access	***Key Access = 1***	***Key Access = 0***
Read Area A	Kd	Kd or Kc
Read Area B	Kc	Kd or Kc
Write Area A	Kd	Kc
Write Area B	Kc	Kc
Debit	Kd or Kc	Kd or Kc
Credit	Kc	Kc

Note:

- *When Key Access is 0, Kd allows updating Secure stored value area.*

Lock Auth (book 0-1, page 0-7, block1, byte 5, bit 1)

Active low

This bit enables to lock the authentication when ISO15693 protocol is used. When ISO14443 type B is used the authentication works.

This bit is updated at boot and for each PageSel command.

IsoB-3 (book 0, page 0, block1, byte 5, bit 2)

Active low

When set to 0 the chip uses the ISO14443-3 type B protocol.

This bit is updates only at boot. If this bit is set, when cannot switch to 14443-2 type B protocol.

2K (book 0-1, page 0, block1, byte 5, bit 4)

Not used in PicoPass 2K

Book (book 0, page 0, block1, byte 5, bit 5)

Not used in PicoPass 2K

16K (book 0-1, page 0, block1, byte 5, bit 7)

Not used in PicoPass 2K

3.1.4 Chip configuration byte

Bit	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
Designation	-	-	-	MulAp	-	-	-	┤

Fig. 5 Chip Configuration byte

Multi Application Identification:

Not used in PicoPass 2K / Bit 4 = 1

Others bits are RFU.

3.1.5 BLOCK WRITE LOCK

This byte manages the block write lock feature

Bit	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
Designation	**RO**	**Block 12**	**Block 11**	**Block 10**	**Block 9**	**Block 8**	**Block 7**	**Block 6**

When a bit is set to zero, the corresponding Block automatically becomes read only.
Setting RO to zero makes the chip whole memory read only.

Examples:
1/ If bit 0, Block 6 = 0, Application Block 6 is in read only mode.
2/ If bit 7, RO = 0, the chip is totally in read only mode.

> *Notes:*
>
> - *To enable reading without authentication on secured pages, user can change RA bit in the* ***Fuses*** *byte.*
> - *When the whole memory is locked, the* ***e-purse*** *cannot be used anymore*

3.1.6 APPLICATION 16-BIT OTP AREA

OTP stands for "One Time Programming".

Block 1 byte number	**1**								**2**							
Bit	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Value	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Each bit can be set to 0 only one time.

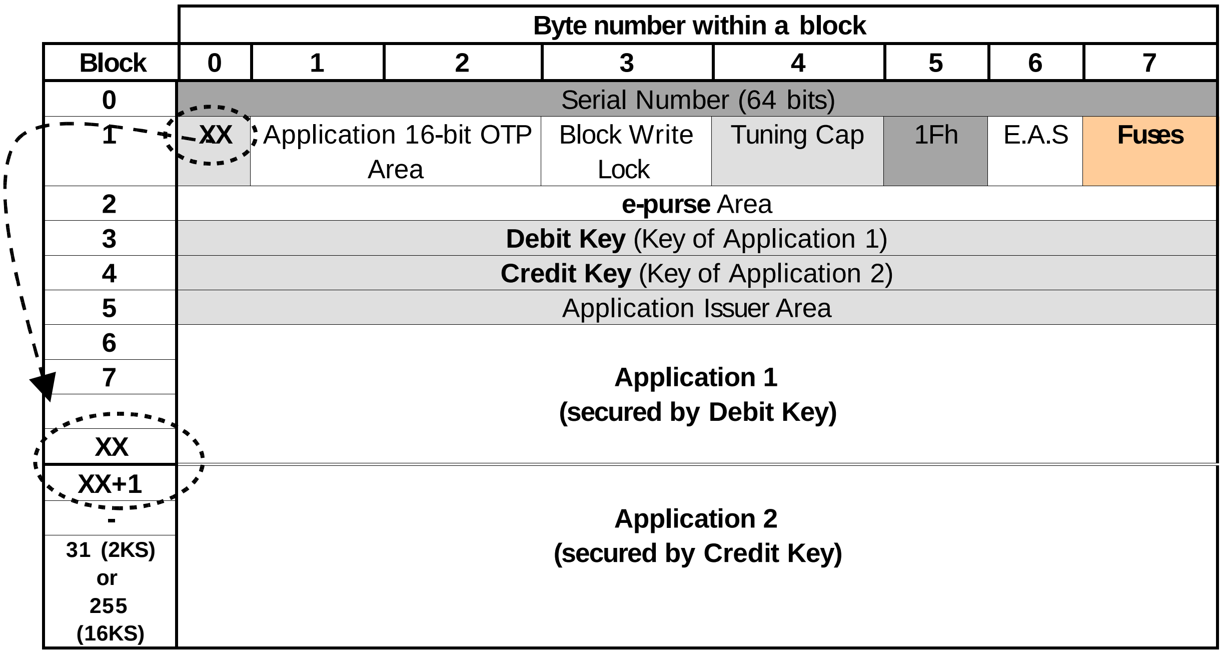
Application example: This area can be used by the application as a 16-bit decrement only counter.

3.1.7 APPLICATIONS LIMIT

This byte defines the limit between the two applications area. The table below shows how the byte 0 of the block 1 can be configured according to the needs of the application.

> *Note: this byte is OTP (one time programming). So you can only set its bits to 0. This implies that you can decrease the limit, but you can never increase it*

To have access in read and write mode into the Application 1 area (respectively Application 2 area), an authentication procedure with Debit Key (respectively Credit Key) must have been performed previously (for further details, please refer to chapter AUTHENTICATION).



	Byte number within a block							
Block	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	Serial Number (64 bits)							
1	XX	Application 16-bit OTP Area		Block Write Lock	Tuning Cap	1Fh	E.A.S	**Fuses**
2	**e-purse** Area							
3	**Debit Key** (Key of Application 1)							
4	**Credit Key** (Key of Application 2)							
5	Application Issuer Area							
6	**Application 1** **(secured by Debit Key)**							
7								
XX								
XX+1	**Application 2** **(secured by Credit Key)**							
-								
31 (2KS) **or** **255** **(16KS)**								

Fig. 6 APPLICATIONS LIMITS

> *<u>Note:</u> For 2KS pages, if Applications Limit equals to 1Fh or more, the application area is made up of 26 blocks protected by Debit Key. If Applications Limit equals to 05h or less, the application area is made up of 26 blocks protected by Credit Key.*

3.2 Application Issuer Area (book 0-1, page 0-7, block 2 or 5)

Depending on the protocol, this block has different functions.

3.2.1 All protocol except ISO 14 443 B - 3

It could be used to recognize and separate different applications for a same customer.
The data stored in this area becomes read-only when the chip is set in application mode.

Data stored in the Application Issuer Area become read only after fuse **Fpers** is set to zero.

3.2.2 ISO14443-3 type B mode: Protocol Info (book 0-1, page 0-7, block5, byte 2-0)

In ISO14443-3 type B mode, this area is reserved to store specific information as shown below.

Block	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
	Protocol Info							AFI

1st byte	***2nd byte***		***3rd***		
b7-b0	**b7-b4**	**b3-b0**	**b7-b4**	**b3-b2**	**b1-b0**
Bit rate	**Max frame size**	**Protocol type**	**FWI**	**ADC**	**FO**

- Bit rate : 0x20 = 424Kbit/s possible from chip to reader
- Max frame size : 0x0 = minimum frame size = 16 bytes max
- Protocol type : 0x0 = PICC not compliant with ISO 14443-4
- FWI = Frame waiting time = 0x6 (chip maximum time to answer is 19.3 ms)
- ADC = Application data coding = 00 (coding is proprietary)
- FO = 00

This field is used during 14443-3 anti-collision for ATQB response.

The data stored in this area becomes read-only when the chip is set in application mode.

3.2.3 AFI (book 0-1, page 0-7, block5, byte 7)

ISO14443-3 type B mode only

Application Family Identifier is compared with the AFI sent by the reader during a REQB/WUPB command for anti-collision.

For single application chip, all AFI of all books/pages have to be the same.

For multi-application, AFI of book0, page 0 has to be 0x00. In this case, chip will answer to and REQB/WUPB whatever AFI is sent by the reader.

3.3 Chip configurations

User's can configure the following features according to its needs:
- Memory organization
- Security
- Protocol

Annex II gives block 1 values for various settings. Reading this block will enable the user to know the configuration of the chip he is communicating with.

- Security

Each page may be secured or not and can be configure independently from the others

- Protocol

Protocols are dedicated to the page that is active. For example, one page (book) may be configure in 15 693 and the next page may work only in 14 443 type B

3.4 Chip personalization

Personalizing the chip is not difficult. Once the definitive settings are defined, user has just to write the correct value in the configuration block.
The main difficulty is to write the new key values. This critical operation is described in the documentation of the personalization kit (Chip personalization application note). More over, a special coupler is needed to calculate the diversified key values that are written in the chip (Personalization couplers).

With PicoPass 2K(S) it is possible to modify the keys even if chip is application mode. This is an option in the Security chip configuration.
Bit Crypt 0 and Crypt 1 of the Fuse byte (configuration block) has to be set both at one.

4 CHIP COMMAND SET

4.1 Presentation

PicoPass chips can respond to coupler commands using different coding:

Standard	Coding
1. ISO 15693-2	Manchester coding.
3. ISO 14443 Type B	BPSK coding

The coding used by the chip to respond is determined according to the value of the command byte. The 1-byte command can be decomposed as follows:

Command format (1 byte)							
7	6	5	4	3	2	1	0
P	M1	M0	K	Instruction			

Fig. 7 COMMAND FORMAT

- Bits 0 to 3: Instruction.

These bits set the instruction as defined in the following table:

Instruction	Hexadecimal value
READ (8 bytes = 1 block)	C
READ4 (32 bytes = 4 blocks)	6
UPDATE (8 bytes = 1 block)	7
READCHECK	8
CHECK	5
ACTALL	A*
ACT	E*
IDENTIFY	C*
SELECT	1*
DETECT	F*
HALT	0*
PAGESEL	4

Fig. 8 INSTRUCTION SET

*: These commands are not valid for ISO 14 443 type B -3 protocol

Note: *The four remaining possible values are RFU (Reserved for Future Use).*

- Bit 4: K.

If this bit equals to one, the READCHECK will use the Credit Key (Kc); if equals to zero, Debit Key (Kd) will be used.

For the other commands this bit is RFU (Reserved for Future Use) and should be set to 0.

- Bit 5 and 6: M0 and M1.

These bits define the coding that the chip will use to answer.

M1	***M0***	***Response data coding if command received in ISO 15693-2***	***Response data coding if command received in ISO 14443 Type B***
0	0	ISO 15693-2 Manchester coding	ISO 14443 Type B (106 kbits/s)
0	1	RFU	ISO 14443 Type B (106 kbits/s)
1	0	ISO 15693-2 Manchester coding	ISO 14443 Type B (423 kbits/s)
1	1	RFU	RFU

Fig. 9 M0 AND M1 BITS

> Notes:
>
> - *The chip automatically responds in ISO14443-2 Type B if the command was send by the reader in ISO 14443-2 Type B format.*
> - *When the chip is personalized in ISO 14443-2 Type A bit coding, M0 & M1 have to be set to "0", otherwise a bad instruction is detected.*
> - *When ISO 15693-2 or ISO 144443-2 Type B protocols are used, if M0 & M1 are set to "1", a bad command is detected.*

- Bit 7: P.

This bit checks the seven bits [Bit6...Bit0] for data integrity, using the following equation:
P = Bit0 ⊕ Bit1 ⊕ Bit2 ⊕ Bit3 ⊕ Bit4 ⊕ Bit5 ⊕ Bit6

⊕ stands for LOGICAL EXCLUSIVE OR.

Example of calculation:
To send a SELECT instruction and to receive the chip answer in ISO 15693-2 Manchester coding, the following command must be sent:

- Bits 0 to 3 : Instruction : 0001
- Bit 4 : K : 0
- Bits 5 and 6 : M0 and M1 : 00 (ISO 15693-2 Manchester coding)
- Bit 7 : P : 0 ⊕ 0 ⊕ 0 ⊕ 1 ⊕ 0 ⊕ 0 ⊕ 0 = 1

	Command SELECT							
Bit	7	6	5	4	3	2	1	0
Value	1	0	0	0	0	0	0	1

⇨ SELECT = 81h.

4.2 Chip command set

4.2.1 ISO 15 693-2 and ISO 14 443 type B -2 Anti-collision

ACTALL

ACTALL wakes up the chips in the field which are not in halted state. The chip then answer a SOF (start of frame) to indicate to the reader that it is in the RF field.

IDENTIFY

IDENTIFY reads the chip Anti-collision Serial Number. If the CRC16 following this response is correct, the chip can then be selected with a command SELECT. Otherwise an ACT command needs to be sent.

SELECT

This command selects the chip with its Anti-collision Serial Number. The chip answers with its Serial Number. Only a selected chip will answer to subsequent commands like READ, UPDATE, etc…

HALT

HALT deselect the chip.
Once the chip is selected and authenticated, an HALT command change the chip state (from SELECTED to HALTED) but does not reset the r/w/e access obtained after a Kc or Kd Authentication.
This means that the chip will not answer to any command except to the SELECT command if it is followed by the chip serial number

4.2.2 ISO 14 443 type B -3 Anti-collision

The following functions are specific to ISO 14 443 type B -3 Anti-collision.

REQ B

The first command to use. It wakes up the chips, and informs them about the number of slot markers that will be used in the anti-collision process.

ATTRIB

This command is used to give to the chip information about the communication (bit rates).

HLTB

This command halts the chip which will not answer anymore to any command.

4.2.3 Chip memory management

PAGESEL

PAGESEL enables to select a page in the selected chip memory and return it configuration block.
Sending a PAGESEL command to the current page reset the current page's cryptographic rights.
Chips with a single page will not answer to this command.

READCHECK (Security command)

This command reads a block and starts an authentication procedure. The chip answer the content of the block pointed by the address, then starts calculation with its algorithm on the return data. The result of this calculation will be compare to the data sent by the coupler with the Check command (see Authentication chapter for more information).
This command may also be used to checked that the answer to coupler command is done by a real chip (i.e. not an emulator)

In the authentication procedure, this is the first instruction to send.
The first READCHECK instruction reset the algorithm core in order to compute the calculation.
The last READCHECK, before a CHECK instruction has to be sent on the **e-purse** block (block 2). (See the Authentication Chapter)

CHECK (Security command)

In the authentication procedure, the CHECK instruction response enables the reader to authenticate the chip.
Challenge in the instruction format is computed by the core algorithm (the CHECK instruction code is not included in the calculation)
Once the chip is authenticated with **Kd**, a **Kd** authentication failure does not reset the rights acquired.
Once the chip is authenticated with **Kc** or **Kd**, a **Kc** authentication failure **reset** the rights acquired.

READ (Read, Read4)

Once the chip is selected and authenticated, READ instructions allow reading the blocks pointed by the address sent with the instruction.
If read is not allowed in the block, chip sends the bits at "1" (bytes at FF).

When a Read4 is performed at the edge of the Applications Limit irrespective of the mapping, if the read access is not allowed the chip responds the bits at "1".

When a Read4 is performed at the end of a page, after reading the last address, the chip restarts from the address 00h of the selected page.

When any of this command is performed on a 2K page, the chip don't take into account the 3 MSB (most significant bits) sent, so the address is always understood between 0h and 1Fh.

UPDATE

Once the chip is selected and authenticated, UPDATE instruction allows updating the addressed memory block.

If UPDATE instruction is not allowed in the block, the chip waits for a new instruction after **Trout.**
If erase is not allowed (fuses block), the chip writes the block without erasing it and returns the results.
The UPDATE Operation code is not included in the signature or CRC calculation.

Programming Time **Tprog** is the following range: 4 to 15 ms

4.2.4 Command set summary

The following table summarizes the different possibilities and their corresponding values…

Command	***Description***					
Protocol used by the coupler	15 693 Level 2	14443B Level 2	14443B Level 2	14443B Level 3	14443B Level 3	
Protocol used by the chip to answer	Manchester *26kbds*	14443B Level 2 *106kbds*	14443B Level 2 *424kbds*	14443B Level 3 *106kbds*	14443B Level 3 *424kbds*	
READ	0C	0C	CC	0C	CC	Read a block in memory at the sent address.
UPDATE	87	87	47	87	47	Erase, write data and verify at the sent address.
READCHECK (1)	88 or 18	88 or 18	48 or D8	88 or 18	48 or D8	Read data at the sent address to be integrated in the authentication with the key selected : 88 or 28 or 48 : Kd (Debit Key) and 18 or B8 or D8 : Kc.(Credit Key).
CHECK (1)	05	05	C5	05	C5	Authenticate using cryptographic algorithm.
PAGESEL	84	84	44	84	44	Select a chip page
READ4	06	06	C6	06	C6	Read 4 blocks at a time
ACTALL	0A	0A	CA	-	-	Separate chips in the field during the anti-collision procedure.
ACT	8E	8E	4E	-	-	Separate active chips in the field during the anti-collision procedure.
IDENTIFY	0C	0C	CC	-	-	Read the anti-collision serial number during the anti-collision procedure.
SELECT	81	81	41	-	-	Select a chip with its anti-collision serial number or select a halted chip with its serial number.
DETECT	0F	0F	CF	-	-	Detect activated EAS chip.
HALT	00	00	C0	-	-	Deselect the chip.
REQB	-		-	05	05	
ATTRIB	-		-	1B	1B	
HLTB	-		-	50	50	

Fig. 10 CHIP COMMAND SET

LSB is transmitted first.

Notes:

1. Chip protocol answer depends on the protocol use for the command.

> *2. The bit4 (K) of the command is actually not used by the chip in most of the instructions (K used only in READCHECK). Nevertheless the only supported values are the ones given in the array above.*

4.3 PicoPass commands format

4.3.1 Byte and bit Orientation

In the chip response, the byte 0 is sent first and the byte 7 is sent last.
Then, for each byte, the Least Significant Bit is transmitted first.

The hex value for the stored data is defined as follows:

	MSB							***LSB***
Bit	7	6	5	4	3	2	1	0
Byte	Hexadecimal value							

The Least Significant Bit (LSB) is transmitted first.

> *Note: MSB stands for Most Significant Bit.*

4.3.2 Commands and answers format for ISO 15 693-2 and IS0 14 443 type B-2 protocols

Length (bytes)					Length (bytes)		
READER COMMAND				**TIME**	**CHIP RESPONSE**		
1	1	2			8	2	
READ	ADDRESS	CRC16		Tout	DATA	CRC16	
1	1	2			32	2	Read and Write commands
READ4	ADDRESS	CRC16		Tout	DATA	CRC16	
1	1	8	4/2		8	2	
UPDATE (3)(4)	ADDRESS	DATA	SIGN/CRC16	Tprog	DATA	CRC16	
1		1			8		
READCHECK		ADDRESS		Tout	DATA		Security commands
1	4	4			4		
CHECK	CHALLENGE	READER SIGNATURE		Tout	CHIP RESPONSE		
1		8			8	2	
SELECT		ASNB (1) or SERIAL NB		Tout	SERIAL NB	CRC16	
1					8	2	
IDENTIFY				Tout	ASNB (1)	CRC16	
1							Anti-collision commands
ACTALL				Tslot	SOF (2)		
1							
ACT				Tslot	SOF (2)		
1							
HALT				Tout	SOF (2)		
1	1	2			8	2	
PAGESEL	Page (0..7)	CRC16		Tout	Block 1	CRC16	
1					8	2	
DETECT				Tout	SERIAL NB	CRC16	EAS command

Fig. 11 COMMAND FORMAT

ISO 15693-2 : Tout = 330 µs, Tprog[1] = 4 to 15 ms, Tslot = 330 µs + (number of slots x 160 µs)
ISO 14443-2 Type A : Tout = 100 µs, Tprog = 4 to 15 ms, Tslot = 100 µs+ (number of slots x 80 µs)
ISO 14443-2 Type B : Tout = 76 µs, Tprog = 4 to 15 ms, Tslot = 119 µs+ (number of slots x 150 µs)

[1]

Notes:

(1) ASNB stands for Anti-collision Serial Number (for further details, please see the Anti-collision chapter)

(2) SOF stands for Start Of Frame (for further details, please refer to chapter 9 BIT AND FRAME CODING).

(3) For secured version, the command UPDATE must be ended by a cryptographic signature calculated with INSIDE Contactless' proprietary algorithm. For unsecured products, this command is ended with a CRC16 which calculation details are available on demand.

(4) This command performs an erase of the block followed by a write of the data.

4.3.3 Commands and answers format for IS0 14 443 type B -3 protocol

Length (bytes)		Length (bytes)
READER COMMAND	**TIME**	**CHIP RESPONSE**

1	1	2				8	2
READ	ADDRESS	CRC_B			Tout	DATA	CRC_B
1	1	2				32	2
READ4	ADDRESS	CRC_B			Tout	DATA	CRC_B
1	1	8	4/0			8	2
UPDATE (3)(4)	ADDRESS	DATA	SIGN/ Empty	CRC_B	Tprog	DATA	CRC_B
1	1	2				8	2
PAGESEL	Page (0..7)	CRC_B			Tout	Block 1	CRC_B

Read and Write commands

1		1		8
READCHECK		ADDRESS	Tout	DATA
1	4	4		4
CHECK	CHALLENGE	READER SIGNATURE	Tout	CHIP RESPONSE

Security commands

1	1	1	2					1	4	4	3
REQB / WUPB	AFI	PARAMETER	CRC_B				Tout	ATQB	PUPI	DATA	PROTOCOL

2	
CRC_B	

1	4	1	1	1	1	4	2		1	2
ATTRIB	PUPI	P1	P2	P3	P4	INF.	CRC_B	Tout	Data	CRC_B
1	1			1						
HTLB	PUPI			CRC_B				Tout	Data	CRC_B

Anti-collision commands

1		8	2
DETECT	Tout	SERIAL NB	CRC16

EAS command

Fig. 12 COMMAND FORMAT

ISO 14443-2 Type B : Tout = 76 µs, Tprog = 4 to 15 ms

Notes:

(1) ASNB stands for Anti-collision Serial Number (for further details, please see the Anti-collision chapter)

(2) SOF stands for Start Of Frame (for further details, please refer to chapter 9 BIT AND FRAME CODING).

(3) For secured version, the command UPDATE must be ended by a cryptographic signature calculated with INSIDE Contactless' proprietary algorithm. For unsecured products, this command is ended with a CRC16 which calculation details are available on demand.

(4) This command performs an erase of the block followed by a write of the data.

4.4 CRC calculation

4.4.1 CRC for ISO 15 693 -2 and 14 443 type B -2

The CRC is 2 bytes long.
To calculate it, don't take the command byte into account.
- Preset value: E0 12
- Polynome : 84 08

Example - for the read command (address 06):
Bytes to send = $0C $06 + CRC
Calculate CRC on $06
The CRC value is: $45 $56

4.4.2 CRC for ISO 14 443 type B -3

The CRC is 2 bytes long.
To calculate it, all the bytes must be taken into account.
- Preset value: FF FF
- Polynome: 84 08

Example - for the read command (address 06):
Bytes to send = $0C $06 + CRC
Calculate CRC on $0C $06
The CRC value is: $2E $3C

4.5 Timings

The following table provides approximate durations of different commands (from first coupler command bit to last chip response bit):

COMMAND	*DURATION (ms)* *ISO 15693-2*	*DURATION (ms)* *ISO 14443-2* *Type B 106k*	*DURATION (ms)* *ISO 14443-2* *Type B 424k*
ACTALL/ACT	1.3 (average time)		
IDENTIFY	4	1.6	0.8
SELECT	6.5	2.4	1.5
READ (8 bytes)	4.2	1.9	1
UPDATE (8 bytes) with cryptographic sign	11.5 to 23.5	7 to 19	6.1 to 18.1
AUTHENTICATION (complete) (1)	8.1	3.4	2.3
HALT	0.8	0.5	0.5
PAGESEL	4.8	1.9	1.1
READ4 (32 bytes = 4 blocks)	12.1	4.2	1.6

Fig. 13 COMMAND TIMING EXAMPLES

Note: (1) For secure chips only

5 INSIDE ANTICOLLISION PROCEDURE

5.1 Presentation

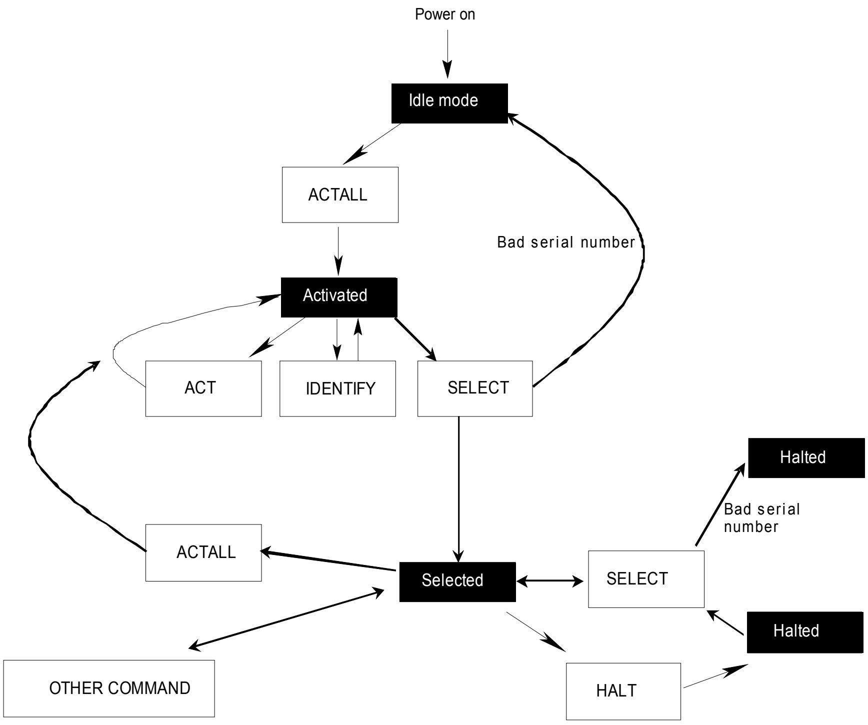


Fig. 14 ANTICOLLISION DIAGRAM

Legend:

Chip Status : ■
Chip Command : □

Direct Selection: If the chip Serial Number is known, it is possible to by-pass the anti-collision procedure and to select the chip directly with the command **SELECT**.
Reselection: After its treatment, a chip can be halted (command **HALT**). It is possible to reselect it by sending a command **SELECT** with its Serial Number. If this latter is erroneous, the chip remains halted.

5.2 Sequence

5.2.1 PRINCIPLE

The anti-collision sequence allows to separate and to treat independently several chips that are present in the same field at the same time.

The Inside's anti-collision procedure uses five commands to perform this feature:

- **ACTALL** activates all chips that are present in the field (wake up) and that have not been halted.

- **ACT** asks all chips to answer with three bits within one of the eight possible slots derived from the Serial Number.

- **IDENTIFY** reads the chip Anti-collision Serial Number. If the CRC16 following this response is correct, the chip can then be selected with a command SELECT. Otherwise another ACT command needs to be sent.

- **SELECT** selects the chip with its Anti-collision Serial Number. The chip answers with its Serial Number. Only a selected chip will answer to subsequent commands like READ, UPDATE, etc…

- **HALT** deselects the chip. A halted chip does not answer to a command ACT. A halted chip can be reselected by sending a command SELECT with its Serial Number or by being removed from the magnetic field (power cut).

The principle is to activate all the chips by sending a command ACTALL.
As soon as one chip or more (impossible to detect) answer, the reader sends a command ACT. Chips that answer during the command ACT are internally halted.

The number of ACT commands needed to be sent after command ACTALL is a function of the number of chips that are supposed to be present in the field. Anti-collision procedure limit regarding the amount of chips that can be separated equals to 2^{64}.

The IDENTIFY command is sent to get the Anti-collision Serial Number of the chip to be selected. If the CRC16 in the chip response is correct, the chip is definitely selected with a command SELECT. If the CRC16 is incorrect, commands ACT must be resent.

At the end of its treatment the chip can be halted with the command HALT.

5.2.2 EXAMPLE

Anti-collision sequence with 3 chips in the field.

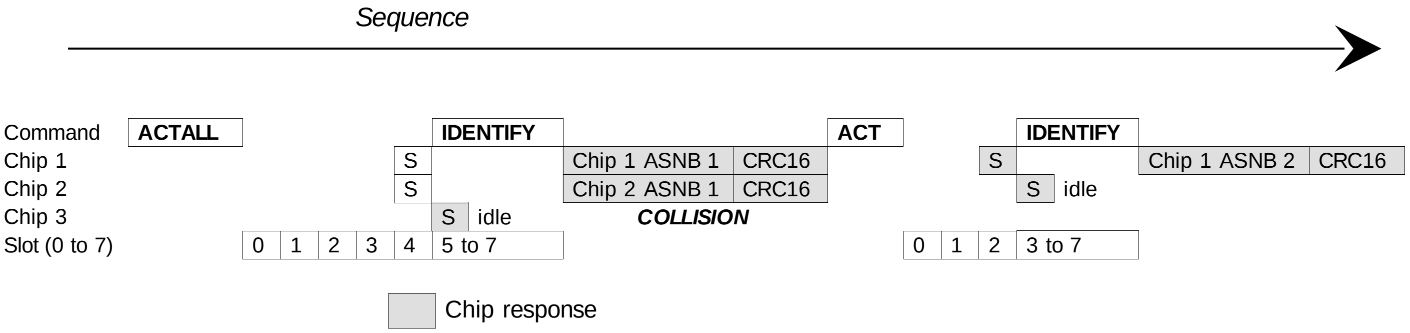


Fig. 15 ANTI-COLLISION EXAMPLE

S stands for Start of frame
ASNB stands for Anti-collision Serial Number.

We assume that the CRC16 received after the command IDENTIFY is correct.
If not, there is a collision and the reader must continue to send an ACT command followed by an IDENTIFY command until the CRC16 is correct.

After this sequence, the reader needs to send a SELECT command with the Chip 1 ASNB 2 Anti-collision Serial Number.
The chip will answer with its correct Serial Number.
The chip becomes selected. You can then send a SELPAGE command to select a page in the chip memory.

5.3 Timings Calculation

Following the communication protocol used, the diagrams below describe the different timings of the anti-collision instruction.

5.3.1 ISO 15693-2 protocol (26 Kbits/s baud rate)

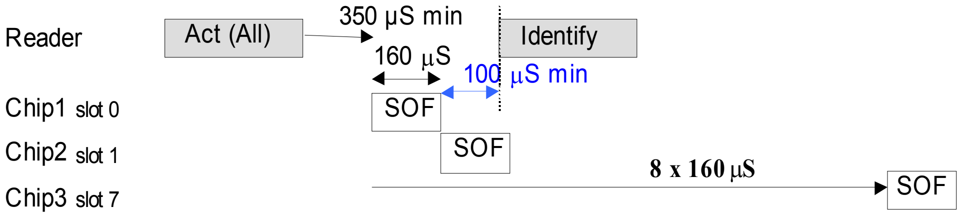


Fig. 16 ISO 15693-2 Anti-collision timings

After an ACTIVATE or ACTIVATE ALL command, a chip response (in SLOT 0) is after 350 µs.
Instruction has to be sent 100 µs minimum after receiving SOF so that the chip is ready to listen to the coupler command. It has to send sent 260 µs maximum so that chip answering in the following slot doesn't understand the coupler command.

Outside the anti-collision sequence, there is no maximum time to send an instruction after Activate(All).
The slot duration is 160 µs.

5.3.2 ISO 14443-B2 protocol (106 or 424Kbits/s baud rate)

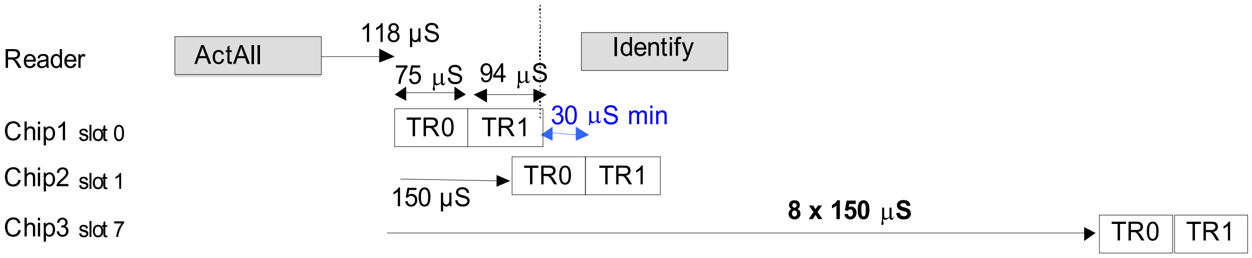


Fig. 17 ISO 14443-B2 Anti-collision timings

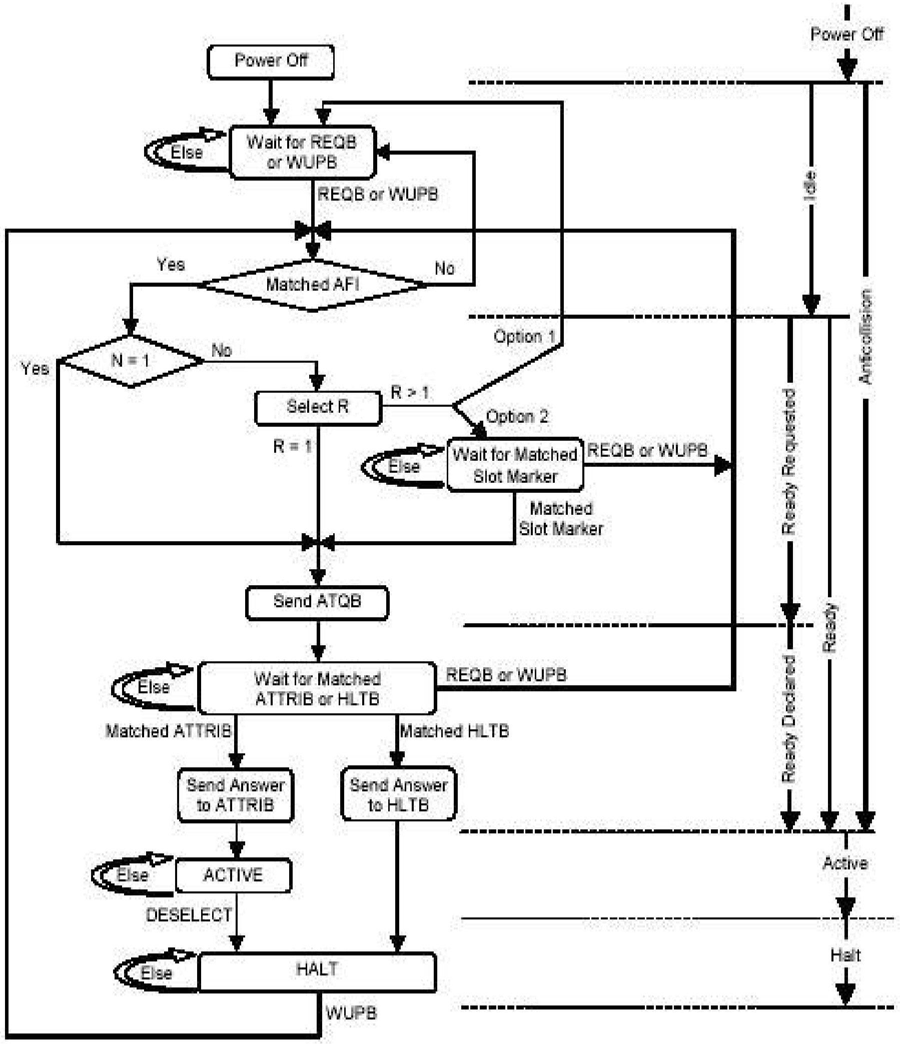
After an ACTIVATE or ACTIVATE ALL command, a chip response (in SLOT 0) is after 118 µs.
Instruction has to be sent 30µs minimum after receiving the end of the TR0 + TR1 data so that the chip is ready to listen to the coupler command. It has to send sent 260 µs maximum so that chip answering in the following slot doesn't understand the coupler command.

Outside the anti-collision sequence, there is no maximum time to send an instruction after Activate(All).
The slot duration is 150 µs.

6 14 443 type B -3 anticollision

6.1 Principle

This anti-collision is the one described in the ISO standard 14 443 type B -3

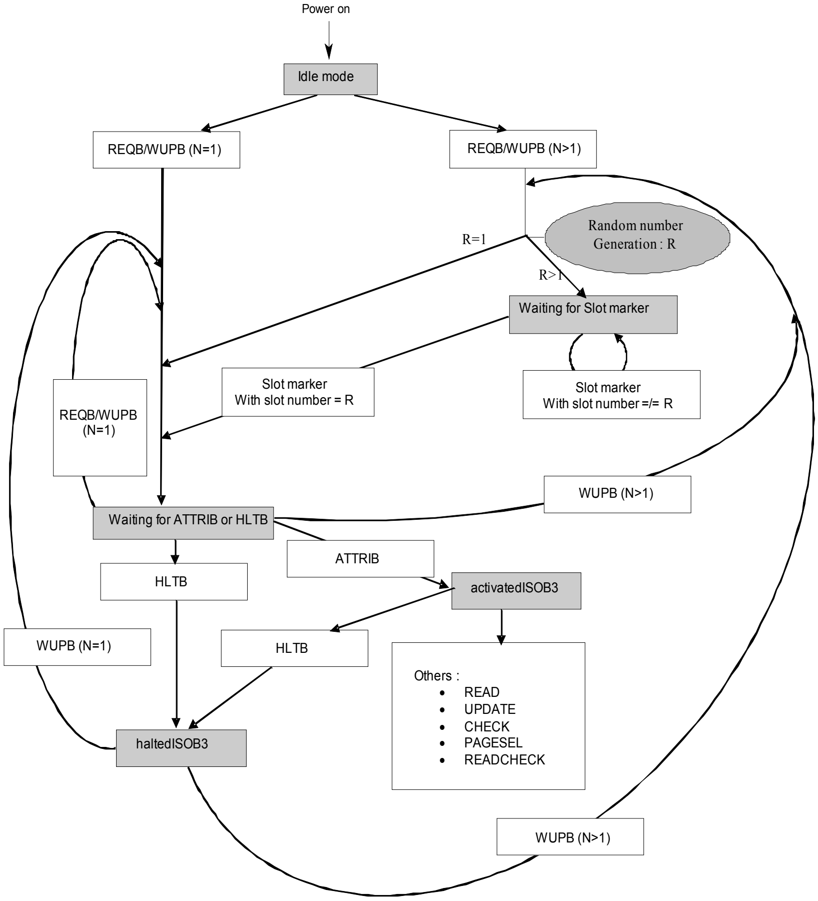


When the chip enters in the field and receives a REQB (after power-on), it compares the AFI (Application family identifier) field contained in REQB command with the value located in Application Issuer Area (address 5, page 0, byte 7). REQB also contains the number of slots (N).

If AFI of REQB matches the chip AFI, chip will check the value of N. If AFI do not match, chip does not respond. In the case where N=1, chip sends back systematically an ATQB response. If N>1, chip calculates a number R (based on its serial number) and is waiting for a SLOT MARKER command with a slot number that matches this number R. When chip receives such a SLOT MARKER, it sends back to the reader an ATQB response. If the number R is 1, the chip sends an ATQB immediately after REQB. This is due to the fact that the moment after REQB is considered as the slot number 1.

Once ATQB is sent, chip is waiting for either an ATTRIB command and thus will be made active (if PUPI of ATTRIB matches the PUPI of the chip) or a REQB/WUPB if a collision occurred.

In case of a collision, the reader starts-over the anti-collision sequence.
Once in active state, the chip is ready to perform read, write or security operations. To halt the chip, the reader sends an HLTB command. If the reader wants to re-activate the chip, it sends a WUPB command (REQB shall be ignored in this state) to rerun an anti-collision sequence.



6.2 ISO 14 443 Type B -3 anti-collision commands and parameters

6.2.1 REQB / WUPB

This command wakes up the chips in the RF field. Only the chips that have the same AFI as the command will be waken up.

Command

CMD	Data		CRC_B
0x05	AFI	P1	
1	1	1	2

Parameters

- AFI :

For AFI coding refer ISO 14443-3 Standard.

- P1

b8	b7	b6	b5	b4	b3	b2	b1
0x0 (RFU)				REQB: 0 WUPB: 1	N (number of slots)		

b1	b2	b3	Number of slots
0	0	0	1
0	0	1	2
0	1	0	4
0	1	1	8
1	0	0	16
1	0	1	RFU
1	1	x	RFU

Chip answer: ATQB

ATQB	**PUPI (serial Nb)**	**App data**	**Protocol info**	**CRC_B**
0x50	4 LSbytes of the serial number	4 MSbytes of the serial number	Bit rate & Max frame & size & Protocol type & FWI & ADC & FO	
1	4	4	3	2

Protocol Info (book 0-1, page 0-7, block5, byte 2-0)

1st byte	2nd byte		3rd		
b7-b0	**b7-b4**	**b3-b0**	**b7-b4**	**b3-b2**	**b1-b0**
Bit rate	**Max frame size**	**Protocol type**	**FWI**	**ADC**	**FO**

- Bit rate : 0x20 = 424Kbit/s possible from chip to reader
- Max frame size : 0x0 = minimum frame size = 16 bytes max
- Protocol type : 0x0 = PICC not compliant with ISO 14443-4
- FWI = Frame waiting time = 0x6 (chip maximum time to answer is 19.3 ms)
- ADC = Application data coding = 00 (coding is proprietary)
- FO = 00

This field is used during 14443-3 anti-collision for ATQB response.

6.2.2 Slot marker

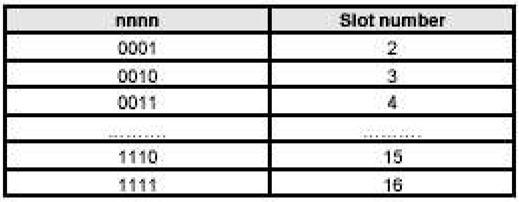
This command has to be sent in the RF field by the reader in order to separate the slot in the RF field.

Command

CMD	*CRC_B*
APn	
1	2

APn = (nnnn 0101), nnnn = coding of slot number

Table 1: Coding of slot number.



nnnn	Slot number
0001	2
0010	3
0011	4
....	....
1110	15
1111	16

Response: ATQB

ATQB	PUPI (serial Nb)	App data	Protocol info	CRC_B
0x50	4 LSbytes of the serial number	4 MSbytes of the serial number	0x200060	
1	4	4	3	2

6.2.3 ATTRIB

This command enables the user to adjust the communication speed between the chip and the reader.

Command

CMD	PUPI	P1	P2	P3	P4	Higher-Layer-INF	CRC_B
0x1D	4 LSbytes of the serial number	0x00	Speed config.	0x00	0x00	4 MSbytes of the serial number	
1	4	1	1	1	1	4	2

Parameters

- **P1 :** set at 0x00
- **P2 :** Enable the user to configure the RF configuration speed

b3	b2	b1	b0
0x0			

b5	b4	
0	0	Reader to chip bit rate is 106 kbit/s

b8	b7	
0	0	Chip to reader bit rate is 106 kbit/s
1	0	Chip to reader bit rate is 424 kbit/s

- **P3 :** set at 0x00
- **P4 :** set at 0x00

Chip answer

Data	CRC_B
0x00	
1	2

6.2.4 HLTB

This command enables the user to stop the chip.

Command

CMD	PUPI	CRC_B
0x50	4 LSbytes of the serial number	
1	4	2

Response

Data	***CRC_B***
0x00	
1	2

7 AUTHENTICATION (SECURED CHIPS ONLY)

7.1 Introduction

In their 2KS secured version, PicoTag and PicoPass chips need to perform an authentication with the reader to allow the execution of the READ and UPDATE commands.
This procedure uses the 64-bit length keys Kc and Kd (respectively Credit Key and Debit Key) based on a proprietary symmetric cryptographic algorithm.

The authentication procedure is totally managed by INSIDE Contactless couplers. To perform this authentication with another coupler you have to use INSIDE Contactless security module. Contact our technical support if more information is needed.

7.2 Principle

- Send a READCHECK command to the chip: it will start its authentication algorithm.

- The **e-purse must be read just before the CHECK command**. This value can change according to the application and is always used by the chip to authenticate the reader. This step of the authentication procedure is obligatory.

- The Command CHECK authenticates the chip. The reader then sends a 32-bit random (CHALLENGE) with its signature (READER SIGNATURE). The chip then checks this signature with its internally calculated one. This authenticates the reader.
  If the READER SIGNATURE is correct, the chip sends its response (CHIP RESPONSE) and the reader compares it with the one expected after its internal calculation. This authenticates the chip.

7.3 Procedure

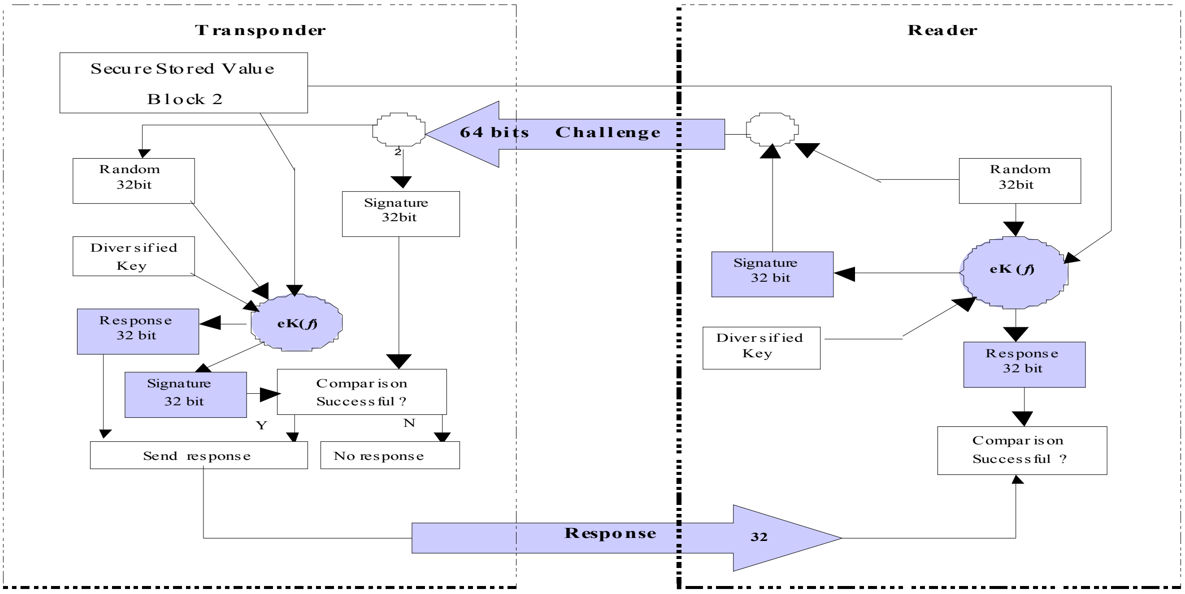


Fig. 18 AUTHENTICATION DIAGRAM

The various step of authentication are:

1. Send the Readcheck command - read address 2
2. Send the Check command with a random (4 bytes) and coupler signature (4 bytes)
3. If coupler signature is correct, chip will answer a new 4 bytes signature that enables the coupler to authenticate the chip.

> ***Note:***
>
> *Several READCHECK Block commands at different addresses can be sent before the command READCHECK on block 2 (**e-purse**). All the responses from the READCHECK Block commands are integrated into the cryptographic calculation.*
>
> *The command READCHECK on block 2 (**e-purse**) is obligatory before the CHECK command to achieve the authentication procedure.*

The coupler diversified key is calculated with the master key (Kd or Kc) and with the chip serial number. It has the same value as the key the chip will use.

8 e-purse (SECURED CHIPS only)

8.1 Principle

The **e-purse** consists in a 16 bit value and a recharging counter (16 bit).

- **Units Value :** It is stored on 16 bits and thus has a maximum value of 65534
- **Recharging counter:** User can set a maximum number of counter recharge. This enables the application issuer to limit card life time, implement a recycle Card-Token. It is coded on 16 bits

Security:
Each operation on **e-purse** value is protected by a secret key. Debit key enables **e-purse** decrease whereas credit key gives total access to it.

- **Authentication:** Before any operation on the **e-purse** you have to perform an authentication with either the debit or the credit keys.
- **Signature:** Each counter modification has to be authenticated by a signature taking into account new counter value, secret key and chip serial number. This ensures a very high security level.

Reliability:
The **e-purse** design makes sure that you have always a reliable value inside. It is made of two 32 bits stages which are written alternatively (see the block mapping below). The old value is erased in the same time the new value is written.
With no communication problem, you can be sure that the new value is correctly written in the memory.
If a problem occurs in processing, you will still have the old value in the memory. Only 2 stages possible: OLD VALUE or NEW VALUE.

8.2 MAPPING AND TERMINOLOGY

We assume that the two-stages principle explained in the previous chapter (7.1 PRINCIPLE) is understood:

	Byte number within a block							
Block	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
2	**VALUE AREA (Stage 1)**				**VALUE AREA (Stage 2)**			

Fig. 19 VALUE AREA MAPPING

Each Value Area can be decomposed into:

- one Recharging Value
- one Debiting Value.

	VALUE AREA			
Byte number	***4 or 0***	***5 or 1***	***6 or 2***	***7 or 3***
Part	**Debiting Value**		**Recharging Value**	
Size (bits)	16		16	

Fig. 20 VALUE AREA DESCRIPTION

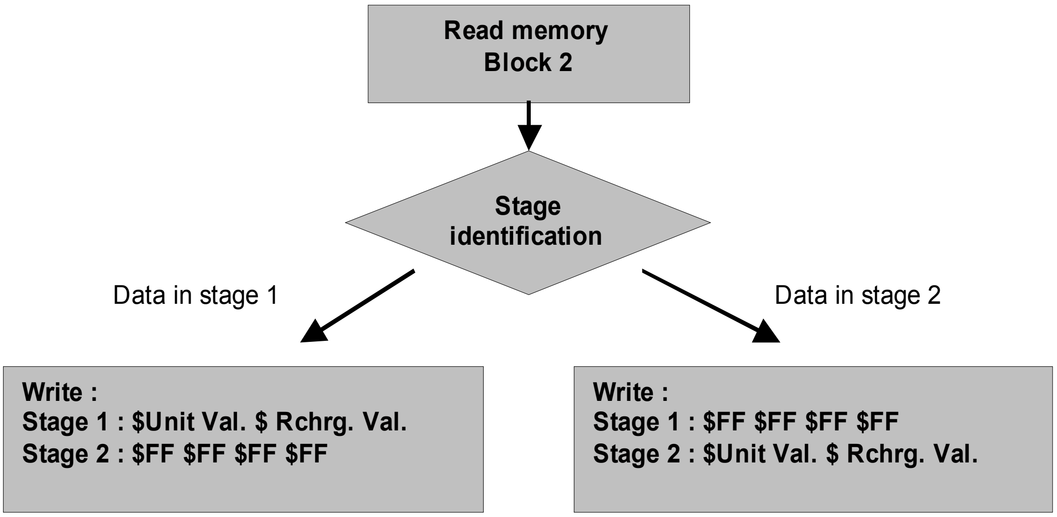
8.3 Recharging and Debiting the Value Area

8.3.1 DEBITING THE VALUE AREA

To debit the Value Area, the following sequence has to be performed:

- Authenticate with Debit Key (Kd). During this procedure, the **e-purse** is read
- Read block 02h to identify the current data stage
- Update block 2 with the new value

Thanks to the store management, the chip will inverse automatically the stage. Thus if you update the stage 1, stage 2 value will be modified and stage 1 will be set to FFFF.


Read memory
Block 2
Stage
identification
Data in stage 1
Data in stage 2
Write :
Stage 1 : $Unit Val. $ Rchrg. Val.
Stage 2 : $FF $FF $FF $FF
Write :
Stage 1 : $FF $FF $FF $FF
Stage 2 : $Unit Val. $ Rchrg. Val.

Rchrg val stands for Recharging counter Value

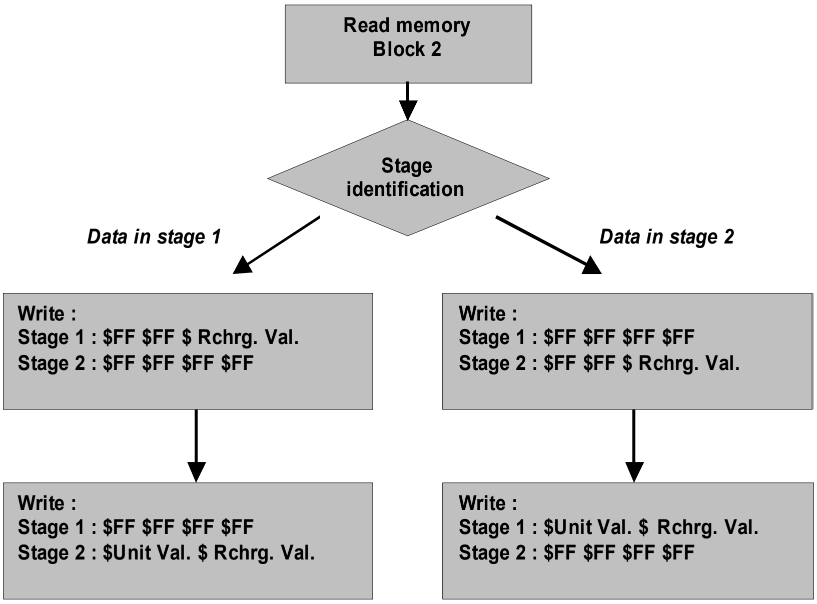
> *Note:*
>
> - *FFFFh is a non valid value for Debiting Value.*
> - *00xxh means that Debiting Value is empty, further debiting is not allowed without a crediting sequence. If xx = 00 then no more crediting is possible.*
> - *If the Signature is incorrect, the **e-purse** is not modified.*
> - *[New Value] must be lower than [Old Value].*

8.3.2 CREDITING THE VALUE AREA

To credit the Value Area, the following sequence has to be performed:

- Authenticate with Credit Key (Kc). During this procedure, the **e-purse** is read.
- Read chip memory block 2 to identify the current stage
- Update the Recharging value.
- Update the Debiting value

You have to take care about the position of the working stage. Just follow the diagram above.


Read memory
Block 2
Stage
identification
Data in stage 1
Data in stage 2
Write :
Stage 1 : $FF $FF $ Rchrg. Val.
Stage 2 : $FF $FF $FF $FF
Write :
Stage 1 : $FF $FF $FF $FF
Stage 2 : $FF $FF $ Rchrg. Val.
Write :
Stage 1 : $FF $FF $FF $FF
Stage 2 : $Unit Val. $ Rchrg. Val.
Write :
Stage 1 : $Unit Val. $ Rchrg. Val.
Stage 2 : $FF $FF $FF $FF

Rchrg val stands for Recharging counter Value

8.3.3 Remarks

- When writing the **e-purse**, keep in mind that you have to write data in the same stage as you read them. Chip will automatically change the stage.

If you read block 2 and data are in stage 1, write the new value in stage 1. The chip automatically writes it in stage 2.

- 0000h means that Recharging Value is empty, further crediting is not allowed.
- If Signature is incorrect, the **e-purse** is not modified and a new authentication procedure must be performed.
- [New Debiting Value] value is unimportant but must be different from FFFFh. Maximum authorized value for Debiting Value is FFFEh.

9 SMART E.A.S

9.1 Presentation

Electronic Article Surveillance is used with its dedicated command: DETECT.
The command DETECT works like the command ACTALL but only chips with activated E.A.S functionality respond to this command.
The chip response is made up of its Serial Number followed by a CRC16.

Command	DETECT	
Chip 1 Response (E.A.S is active)	Chip 1 Serial Number	CRC16
Chip 2 Response (E.A.S is inactive)	No response	

If at least two chips respond to the command the CRC16 is incorrect and an anti-collision procedure with command ACT can be processed.
After this procedure, the chip can be selected by use of the command SELECT and treated if necessary.

The others chips whose EAS is not activated do not respond, and go back to IDLE mode.
The E.A.S detection is described below:

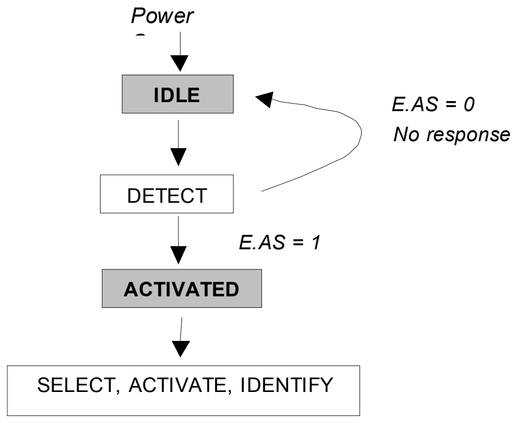


Fig. 5 E.A.S Detection

> ***Note:*** ***In case of fast E.A.S detection, the anti-collision procedure does not need to be implemented. Even if there is a collision and an incorrect CRC16, the reader knows that there are chips in its field.***

9.2 E.A.S activation and deactivation

According to the E.A.S byte value (block 1, byte 6), the E.A.S functionality is active or not.

- Write $7F to activate the EAS feature.
- Write $FF to deactivate the EAS feature.

<u>Remark:</u> When delivered, E.A.S chip is not activated (E.A.S byte equals to FFh).

10 PICOTAG and PICOPASS 15693-2 BIT AND FRAME CODING

This section covers some aspects of the ISO 15693-2 standard.
For modulation and further details, please refer to the standard.

10.1 Reader to chip

10.1.1 BIT CODING: 1 OUT OF 4

This coding defines two bits at a time.

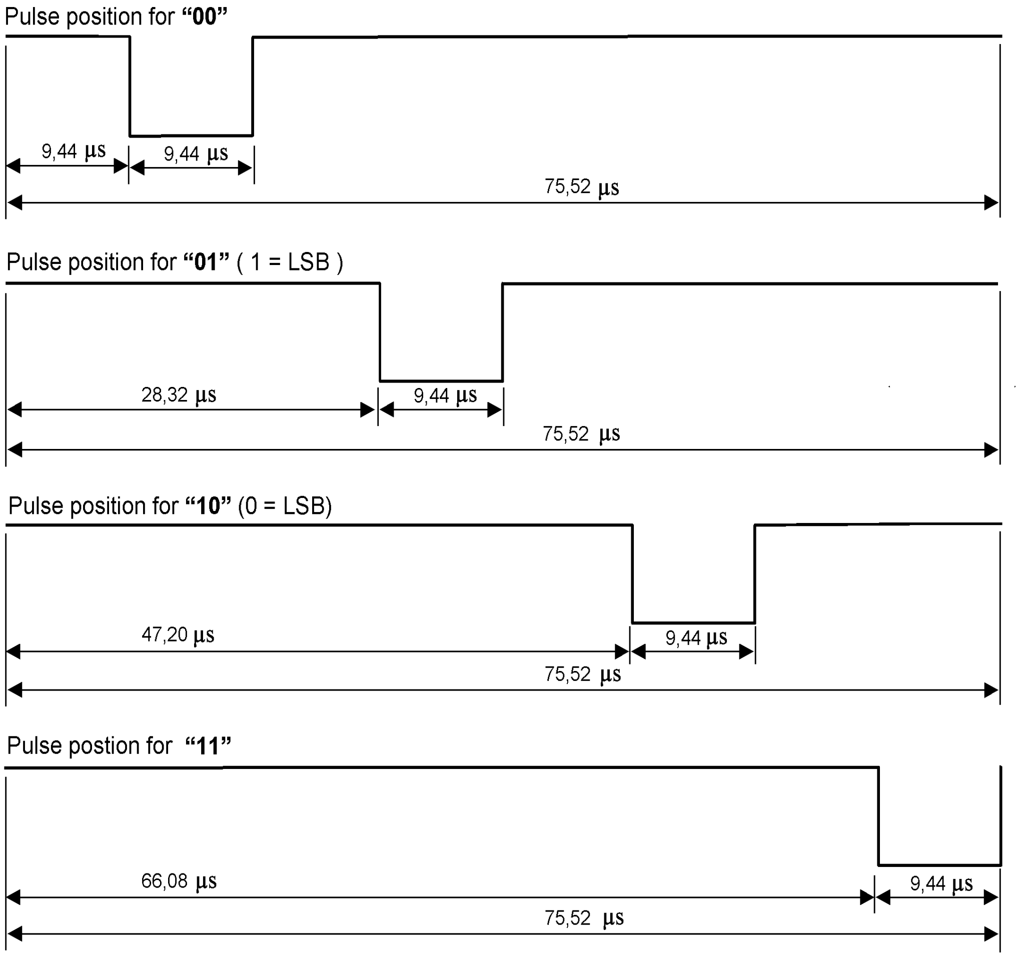

Pulse position for **“00”**
9,44 µs
9,44 µs
75,52 µs
Pulse position for **“01”** (1 = LSB)
28,32 µs
9,44 µs
75,52 µs
Pulse position for **“10”** (0 = LSB)
47,20 µs
9,44 µs
75,52 µs
Pulse postion for **“11”**
66,08 µs
9,44 µs
75,52 µs

Fig. 21 1 OUT OF 4 CODING

Example: The following figure shows the transmission of E1h by the reader:

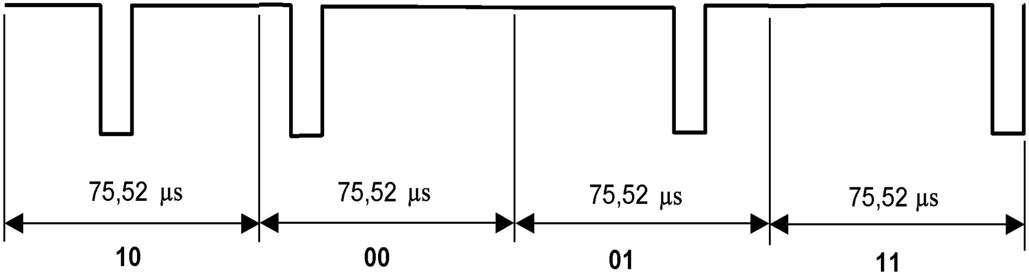


Fig. 22 E1h CODING

Notes :

LSB is transmitted first.

1 out of 256 coding is not supported in this version of the chip.

10.1.2 FRAME

Frames must be delimited by a start of frame (SOF) and an end of frame (EOF) as shown below:

SOF	DATA	EOF

The chip is ready to receive a frame after 100 µs of activation by the powering field.
The chip is ready to receive a frame from the reader 300 µs after having sent a frame to the reader.

The following diagram describes SOF:

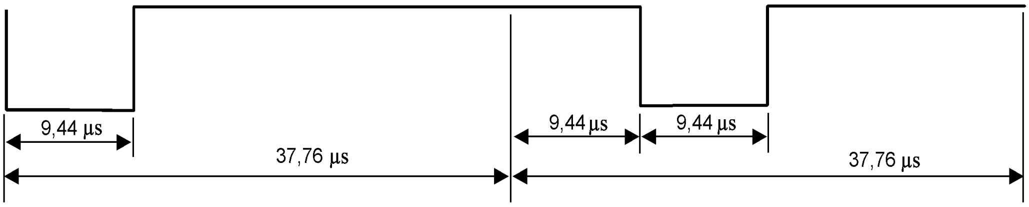


Fig. 23 READER TO CHIP START OF FRAME

The following diagram describes EOF:

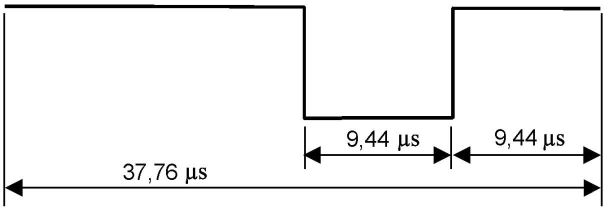


Fig. 24 READER TO CHIP END OF FRAME

10.2 Chip to reader

10.2.1 BIT CODING: Manchester

According to the format of the command (refer to chapter 4 CHIP COMMAND SET for further details), the chip responds using Manchester coding.

MANCHESTER WITH 423.75 KHz SUBCARRIER (8 PULSES)

The two following figures show the logic 0 and the logic 1 coding:

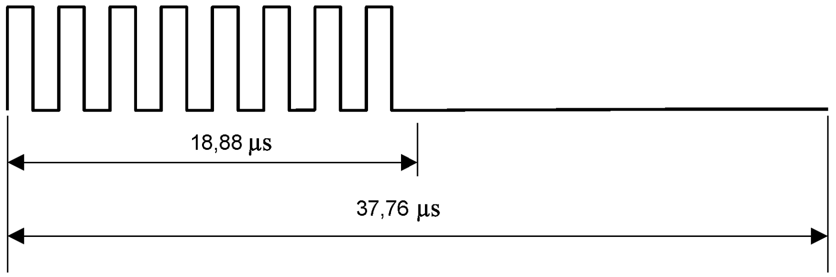


Fig. 25 CHIP TO READER MANCHESTER CODING (LOGIC 0)

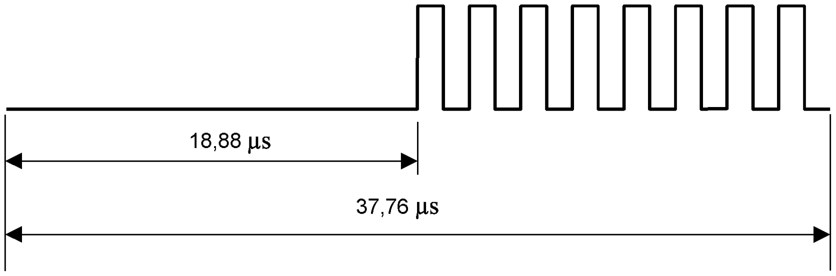


Fig. 26 CHIP TO READER MANCHESTER CODING (LOGIC 1)

10.2.2 FRAME

Frames must be delimited by a start of frame (SOF) and an end of frame (EOF) as shown below:

SOF	DATA	EOF

The following diagram describes SOF in the case of Manchester coding:

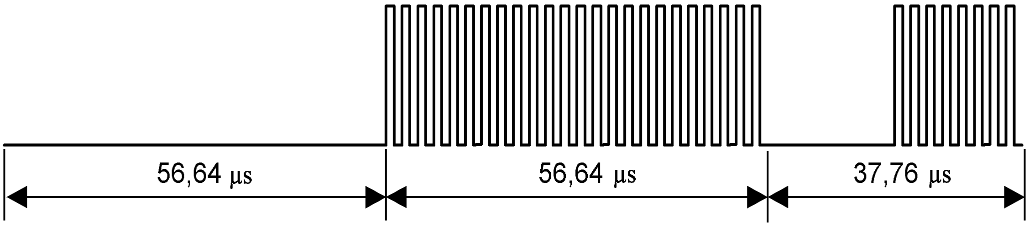


Fig. 27 CHIP TO READER START OF FRAME (Manchester)

Unmodulated time of 37.76 µs, logic 1, 16 pulses of 423.75 KHz, logic 1.

The following diagram describes EOF in the case of Manchester coding:

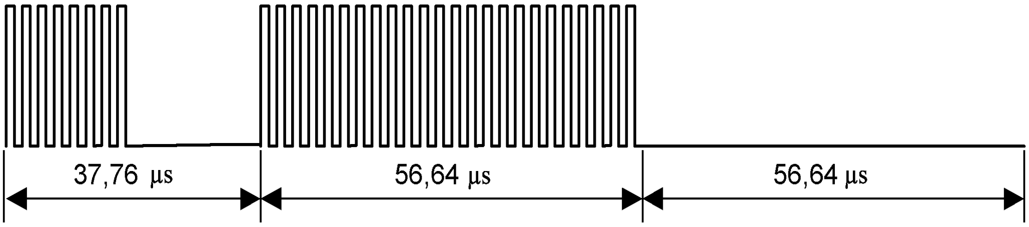


Fig. 28 CHIP TO READER END OF FRAME (Manchester)

Logic 0, 16 pulses of 423.75 KHz, logic 0, unmodulated time of 37.76 µs.

11 PICOPASS ISO 14443 Type B Bit and frame coding

The data bit rate is 106 Kbits/s from the reader to the chip.
According to M1 & M0 the data bit rate from the chip to the reader is 106 Kbits/s or 424 Kbits/s.
Communication between the chip and the reader takes place via ASK 10% amplitude modulation of the RF operating field.

11.1 Character transmission format

Bytes are transmitted and received between chip and reader by characters as follows:

- 1 start bit at logic “0”
- 8 data bits transmitted LSB first
- 1 stop bit at logic “1”

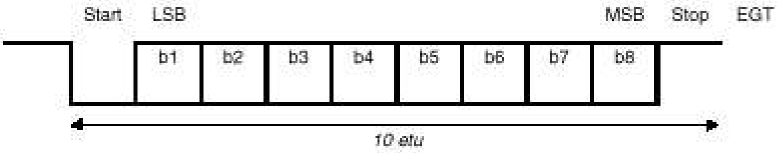


Fig. 29 Character format

Character separation

A character is separated from the next one by the extra guard time EGT.
The EGT between 2 consecutive characters sent by the reader to the chip is from 0 and 57 µs.
The EGT between 2 consecutive characters sent by the chip to the reader is 0 µs.

Note: This is no EGT between the last character and an EOF.

11.2 Frame format

The chip and the reader send characters as a frame. This frame is normally delimited by SOF and EOF.

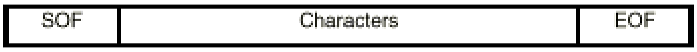


Fig. 30 Character format

11.2.1 SOF (Start Of Frame)

The SOF is composed of:

- One falling edge

- Followed by 10 *etu*[2] with a logic “0”
- Followed by one single rising edge located anywhere within the following *etu*
- Followed by at least 2 *etu* (but no more than 3 *etu*) with a logic “1”.

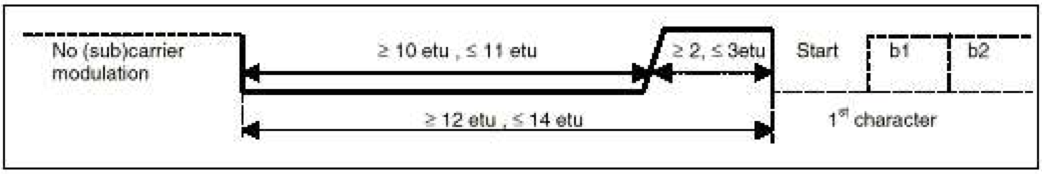


Fig. 31 SOF format

> *Note:*
>
> *The chip range goes from 9 to 12 etu low, and 1.5 to 3.5 etu high.*

11.2.2 EOF (End Of Frame)

The EOF is composed of:

- One falling edge
- Followed by 10 *etu* with logic”0”
- Followed by one single rising edge located anywhere within the following *etu*.

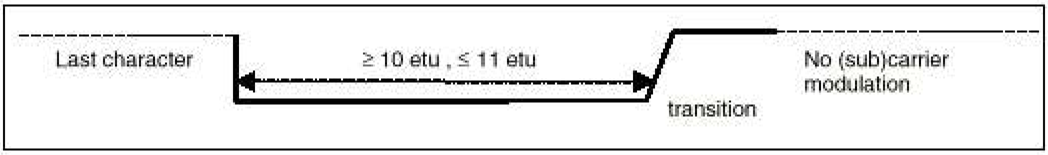


Fig. 32 EOF format

> *Note:*
>
> *The chip range goes from one to 12 etu low.*

11.3 Timing before the chip SOF

The chip starts the communication after a reader data transmission. It respects the following timing:

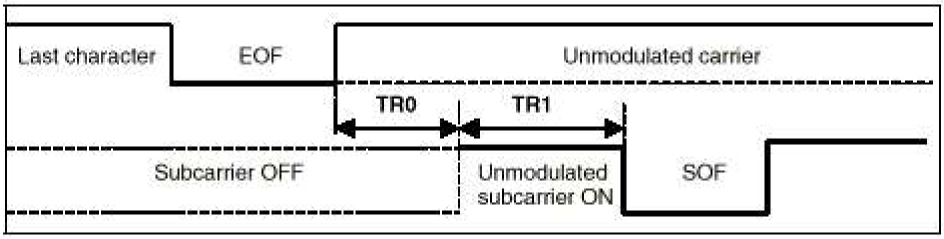


Fig. 33 Timing before the chip SOF

The **TR0** and **TR1** timings are, irrespective the chip response baud rate :

- TR0 is greater than 64 /Fs (76 µs) and the maximum value is 256/Fs[3].
- TR1 is greater than 80 /Fs (95 µs) and the maximum value is 200/Fs.

[2] *Etu* for Elementary Time Unit (128/Fc) = 9.44 µs

[3] Fs for Frequency Sub carrier = Fc/16 = 847.5 kHz.

11.4 Timing after the chip EOF

The reader starts the communication after a chip data transmission and EOF. It respects the following timing:

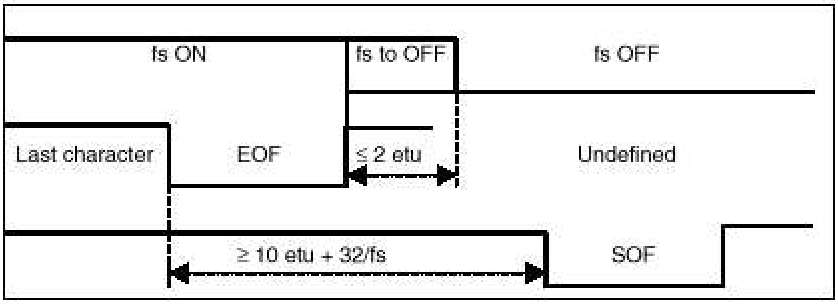


Fig. 34 Timing after the chip EOF

The chip subcarrier is Off the transmission of the EOF. The subcarrier signal is:

- Not stopped before the end of EOF
- Stopped no later than 2 *etu* after the end of EOF.

⇒ When the chip response baud rate is 106 Kbits/s, this time is 1 etu (9.44 µs)
⇒ When the chip response baud rate is 424 Kbits/s, this time is 2 etu (4.72 µs)

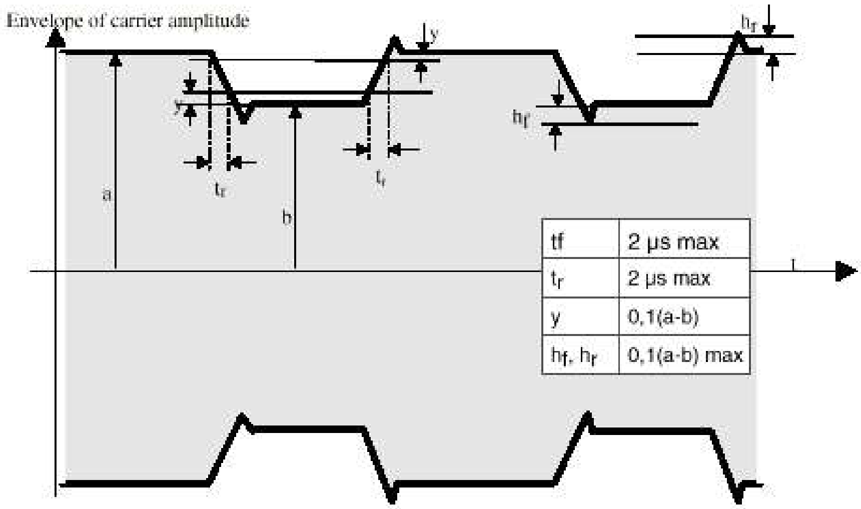
The minimum delay between the chip EOF start (falling edge) and the reader SOF start (falling edge) is:

- When the chip response baud rate is 106 Kbits/s, 10 *etu* + 32/Fs =132µs.
- When the chip response baud rate is 106 Kbits/s, 10 *etu* + 32/Fs =61.3µs.

11.5 Reader to chip bit coding

The data bit rate for the transmission is Fc/128 (106 Kbits/s).
Communication between reader and chip takes place via ASK 10% amplitude modulation of the RF operating field.
The modulation index is a minimum of 8% and a maximum 14%.
The bit coding format is NRZ-L with logic levels defined as follows:

- Logic “1” carrier high field amplitude.
- Logic “0” carrier low field amplitude.



tf	2 µs max
t_r	2 µs max
y	0,1(a-b)
h_f, h_r	0,1(a-b) max

Fig. 35 Reader to chip bit coding

11.6 Chip to reader bit coding

The data bit rate for the transmission is nominally Fc/128 (106Kbits/s) and according to **M0** and **M1** coding Fc/32 (424 Kbits/s)
The chip is able to communicate to the reader via an inductive coupling area where the energizing field is loaded to generate a subcarrier with frequency Fs (Fc/16: 847.5 KHz)
The chip generates a subcarrier only when data is to be transmitted.
Bit coding is NRZ-L where a change of logic state is denoted by a phase shift (180°) of the subcarrier.
The initial phase state $\varnothing_0$ of the subcarrier is defined as a logical “1” so that the first place transition represents a change from logical “1” to logical “0”.
Then the logic state is defined:

$\varnothing_0$	Logical state 1
$\varnothing_0$ **+180°**	Logical state 0

The subcarrier is BPSK modulated as described below:

- When the chip response baud rate is 106 kbit/s, the bit period is 8 subcarrier cycles.
- When the chip response baud rate is 424 kbit/s, the bit period is 2 subcarrier cycles.

Below is detailed an example of data coding:

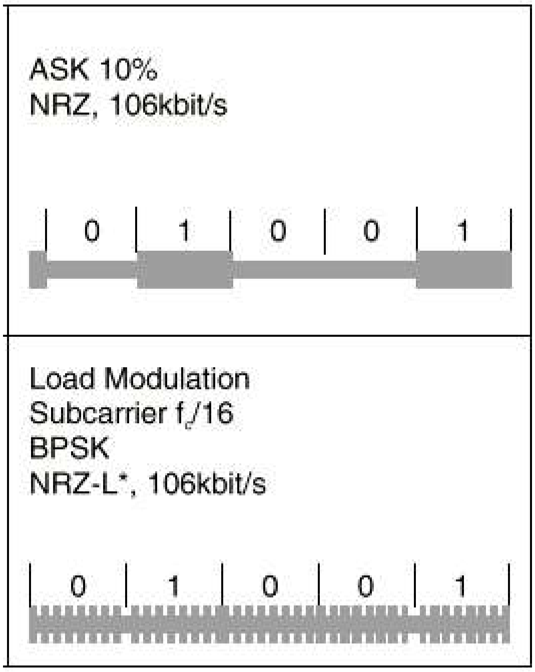


Fig. 36 Reader and chip bit coding for ISO 14443 Type B

12 PAD OUT

To obtain the corresponding datasheet (WF158H2KS), please contact our technical service.

INSIDE technical support :
e-mail : techsupport@insidefr.com
Tel : +33 - 442 39 63 00

13 ANNEXES

13.1 Memory Access summary

The tables on the following pages sum up the memory access function of the different chip modes:

13.1.1 Secured chips

- Write means set a bit to 0
- Erase means set a bit to 1.

			Personalization mode			***Application mode***		
Area		***Size (bits)***	**Read**	**Write**	**Erase**	**Read**	**Write**	**Erase**
Serial Number		*64*	✓	⦸	⦸	✓	⦸	⦸
Configuration block	**Fuses**	*8*	✓	✓ (2a)	⦸	✓	✓ (2b)	⦸
	EAS	*8*	✓	✓ (2a)	✓ (2a)	✓	✓ (2b)	✓ (2b)
	Tuning Cap	*8*	✓	⦸	⦸	✓	⦸	⦸
	Block Write Lock	*8*	✓	✓ (2a)	⦸	✓	✓ (2b)	⦸
	Application 16-bit OTP Area	*16*	✓	✓ (2a)	⦸	✓	✓ (2b)	⦸
	Applications Limit	*8*	✓	✓ (2a)	⦸	✓	⦸	⦸
e-purse		*64*	✓	✓ (2a)	✓ (2a)	✓	✓ (3)	⦸
Debit and Credit Key		*128*	⦸	✓ (2a)	✓ (2a)	⦸	✓ (6)	✓ (6)
Application Issuer Area		*64*	✓(1)	✓ (2a)	✓ (2a)	✓	⦸	⦸
Application Area		*1664 (2K)*	✓(1)	✓ (2a)	✓ (2a)	✓ (4)	✓ (5)	✓ (5)

Fig. 37 MEMORY ACCESS (1)

Notes:

(1): After a successful authentication with Kd.

(2a): After a successful authentication with Kd and a correct cryptographic signature.

(2b): After a successful authentication with Kd or Kc, a correct cryptographic signature and if Read Only bit (RO) is not set to 0.

(3) : After a successful authentication with Kd or Kc, a correct cryptographic signature, according to the new value to be written (for further details, please refer to chapter ***e-purse****) and if Read Only bit (RO) is not set to 0.*

(4): After a successful authentication with Kd or Kc according to Applications Limit value.

(5): After a successful authentication with Kd or Kc according to Applications Limit value, a correct cryptographic signature, and if Read Only bit (RO) is not set to 0.

(6): If Crypt1=Crypt0=1. If Read Only bit (RO) is not set to 0, a successful authentication with Kd enables to change Kd, and a successful authentication with Kc enables to change Kc.

Kd stands for Debit Key, Kc for Credit Key and Kt for Transport Key.

13.1.2 Non secure chips

To write a new byte in the memory chip makes in fact two operations: it erases then writes the memory.

- Write means set a bit to 0
- Erase means set a bit to 1.

In some part of the memory it may be possible to write but not erase bits (example: OTP area).

			Personalization mode			Application mode		
Area		Size (bits)	Read	Write	Erase	Read	Write	Erase
Serial Number		64						
Configuration block	Fuses	8		✓ (1)			✓ (1)	
	EAS	8		✓ (1)			✓ (1)	
	Tuning Cap	8						
	Block Write Lock	8		✓ (1)			✓ (1)	
	Application 16-bit OTP Area	16		✓ (1)			✓ (1)	
Application Issuer Area		64		✓ (1)	✓ (1)			
Application Area		1856		✓ (1)	✓ (1)		✓ (1)	✓ (1)

Fig. 38 MEMORY ACCESS (2)

Notes:

(1) : If corresponding Block Write Lock fuse is not blown and if Read Only bit (RO) is not set to 0.

To our valued customers

We constantly strive to improve the quality of all our products and documentation. We have spent an exceptional amount of time to ensure that this document is correct. However, we realize that we may have missed a few things. If you find any information that is missing or appears in error, please use the contact section below to inform us. We appreciate your assistance in making this a better document.

For further information, do not hesitate to contact us:

11A, Parc Club du Golf
13856 Aix-en-Provence Cedex 3 France
Tel : +33 (0)4 42 39 63 00
Fax : +33 (0)4 42 39 63 19
http ://www.insidefr.com
E-mail : techsupport@insidefr.com