MF1PLUSx0y1

Mainstream contactless smart card IC for fast and easy solution development

Rev. 1.4 — 25 March 2009
163714

Objective data sheet
SECURED, STRICTLY CONFIDENTIAL INFORMATION

1. General description

MIFARE Plus brings benchmark security to the mainstream contactless smart card applications with the possibility to seamlessly upgrade existing infrastructure and services with minimum effort.

It is the only mainstream smart card compatible with MIFARE 4K (MF1ICS70), MIFARE 1K (MF1ICS50) and MIFARE Mini (MF1ICS20), offering to pre-issuance of cards prior to Infrastructure security upgrades. After the security upgrade MIFARE Plus uses AES (advanced encryption standard) for authentication, data integrity and encryption. MIFARE Plus is based on open global standards for both air interface and cryptographic methods in the highest security level.

MIFARE Plus is available in two versions: MIFARE Plus S (MF1SPLUSx0y1), the standard version for straight forward migration of MIFARE Classic systems. It is configured to offer high data integrity. The MIFARE Plus X (MF1PLUSx0y1, described within this document) offers more flexibility to optimize the command flow for speed and confidentiality. It offers a rich feature set including proximity checks against relay attacks.

2. Features

- 2 or 4 KB EEPROM
- Simple fixed memory structure compatible with MIFARE Mini, MIFARE 1K, MIFARE 4K
- Memory structure identical to MIFARE 4K (sectors, blocks)
- Access conditions freely configurable
- Support of ISO/IEC 14443-A unique serial number (4 or 7 byte), support optional of random IDs
- Multi-sector authentication, Multi-block read and write
- AES used for authenticity, confidentiality and integrity
- Anti-tear function for writing AES keys
- Keys can be stored as MIFARE CRYPTO1 keys (2 x 48 bit per sector) or as AES keys (2 x 128 bit per sector)
- Full virtual card concept
- Proximity check
- Communication speed up to 848 kbit/s
- Number of single write operations: 200,000 typical
- Common Criteria Certification: EAL4+

3. Applications

- Public transportation
- Access management
- Electronic toll collection
- Car parking
- School and campus cards
- Employee cards
- Internet cafes
- Loyalty

4. Ordering information

Table 1. Ordering information

Type number	Package			
	Commercial Name	Name	Description	Version
MF1PLUS8001DUD/01	FFC	-	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format) see Section 7 and Section 8, 4K EEPROM, 7 byte UID, 'L1 card'	-
MF1PLUS8001DA4/01	MOA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape, 4K EEPROM, 7 byte UID, 'L1 card'	SOT500-2
MF1PLUS8011DUD/01	FFC	-	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format) see Section 7 and Section 8, 4K EEPROM, 4 byte UID, 'L1 card'	-
MF1PLUS8021DUD/01	FFC	-	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format) see Section 7 and Section 8, 4K EEPROM, 4 byte UID, UID0=xF according to ISO 14443-3, 'L1 card'	-
MF1PLUS8011DA4/01	MOA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape, 4K EEPROM, 4 byte UID, 'L1 card'	SOT500-2
MF1PLUS8021DA4/01	MOA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape, 4K EEPROM, 4 byte UID, UID0=xF according to ISO 14443-3, 'L1 card'	SOT500-2
MF1PLUS6001DUD/01	FFC	-	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format) see Section 7 and Section 8, 2K EEPROM, 7 byte UID, 'L1 card'	-
MF1PLUS6001DA4/01	MOA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape, 2K EEPROM, 7 byte UID, 'L1 card'	SOT500-2
MF1PLUS6011DUD/01	FFC	-	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format) see Section 7 and Section 8, 2K EEPROM, 4 byte UID, 'L1 card'	-

Table 1. Ordering information *...continued*

Type number	Package			
	Commercial Name	Name	Description	Version
MF1PLUS6021DUD/01	FFC	-	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format) see Section 7 and Section 8, 2K EEPROM, 4 byte UID, UID0=xF according to ISO 14443-3, 'L1 card'	-
MF1PLUS6011DA4/01	MOA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape, 2K EEPROM, 4 byte UID, 'L1 card'	SOT500-2
MF1PLUS6021DA4/01	MOA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape, 2K EEPROM, 4 byte UID, UID0=xF according to ISO 14443-3, 'L1 card'	SOT500-2
MF1PLUS8001DUD/11	FFC	-	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format) see Section 7 and Section 8, 4K EEPROM, 7 byte UID, no security level 1, 2, 'L3 card'	-
MF1PLUS8001DA4/11	MOA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape, 4K EEPROM, 7 byte UID, no security level 1, 2, 'L3 card'	SOT500-2
MF1PLUS6001DUD/11	FFC	-	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format) see Section 7 and Section 8, 2K EEPROM, 7 byte UID, no security level 1, 2, 'L3 card'	-
MF1PLUS6001DA4/11	MOA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape, 2K EEPROM, 7 byte UID, no security level 1, 2, 'L3 card'	SOT500-2

5. Block diagram

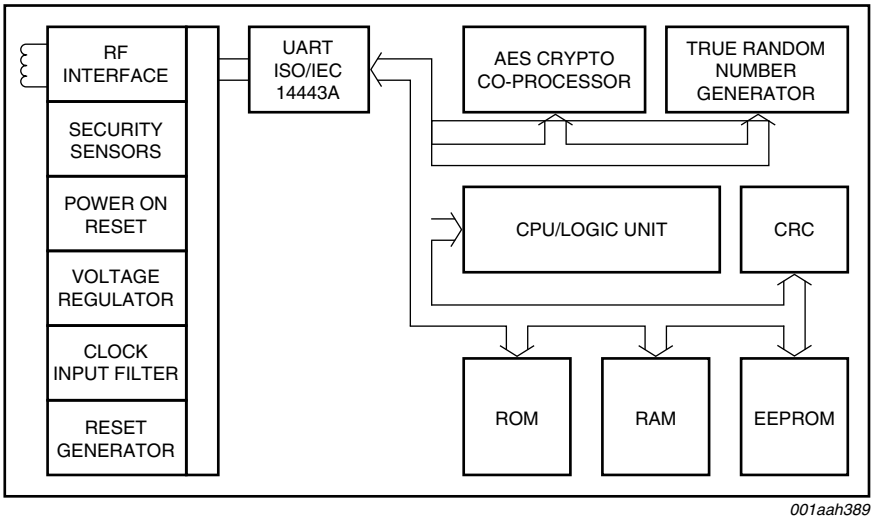


Fig 1. Block diagram

6. Pinning information

6.1 Smart card contactless module

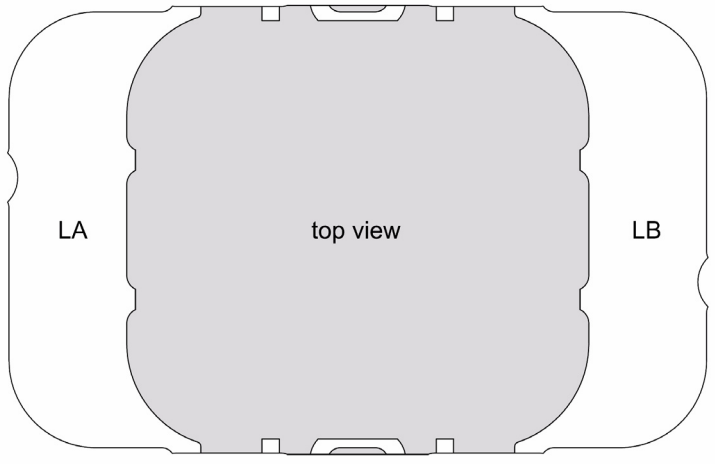


Fig 2. Contact assignments for SOT500-2 (MOA4)

Table 2. Bonding pad assignments to smart card contactless module

Contactless interface module		MF1PLUSx0y1DA4/01
Antenna contacts	**Symbol**	**Description**
LA	LA	Antenna coil connection LA
LB	LB	Antenna coil connection LB

7. Mechanical specification

7.1 Wafer

- Diameter: 8”, 205 mm typical
- Thickness: 120 μm ± 15 μm
- Flatness: not applicable
- PGDW: 18482

7.2 Wafer backside

- Material: Si
- Treatment: ground and stress relieve
- Roughness: R_a max 0.2μm

  R_t max 2μm

7.3 Chip dimensions

- Chip size: 1.201 x 1.250 mm
- Scribe lines: x-line: 15 μm

  y-line: 15 μm

7.4 Passivation

- Type: sandwich structure
- Material: Nitride
- Thickness: 1.75μm

7.5 Au bump

- Bump material: > 99.9% pure Au
- Bump hardness: 35 – 80 HV 0.005
- Bump shear strength: > 70 MPa
- Bump height: 18 μm
- Bump height uniformity:
  - within a die: ± 2 μm
  - within a wafer: ± 3 μm
  - wafer to wafer: ± 4 μm
- Bump flatness: ± 1.5 μm
- Bump size:
  - LA, LB: 69 x 69μm
  - TP1;TP2;VSS: 58 x 58μm
- Bump size variation: ± 5 μm

- Under bump metallization: sputtered TiW

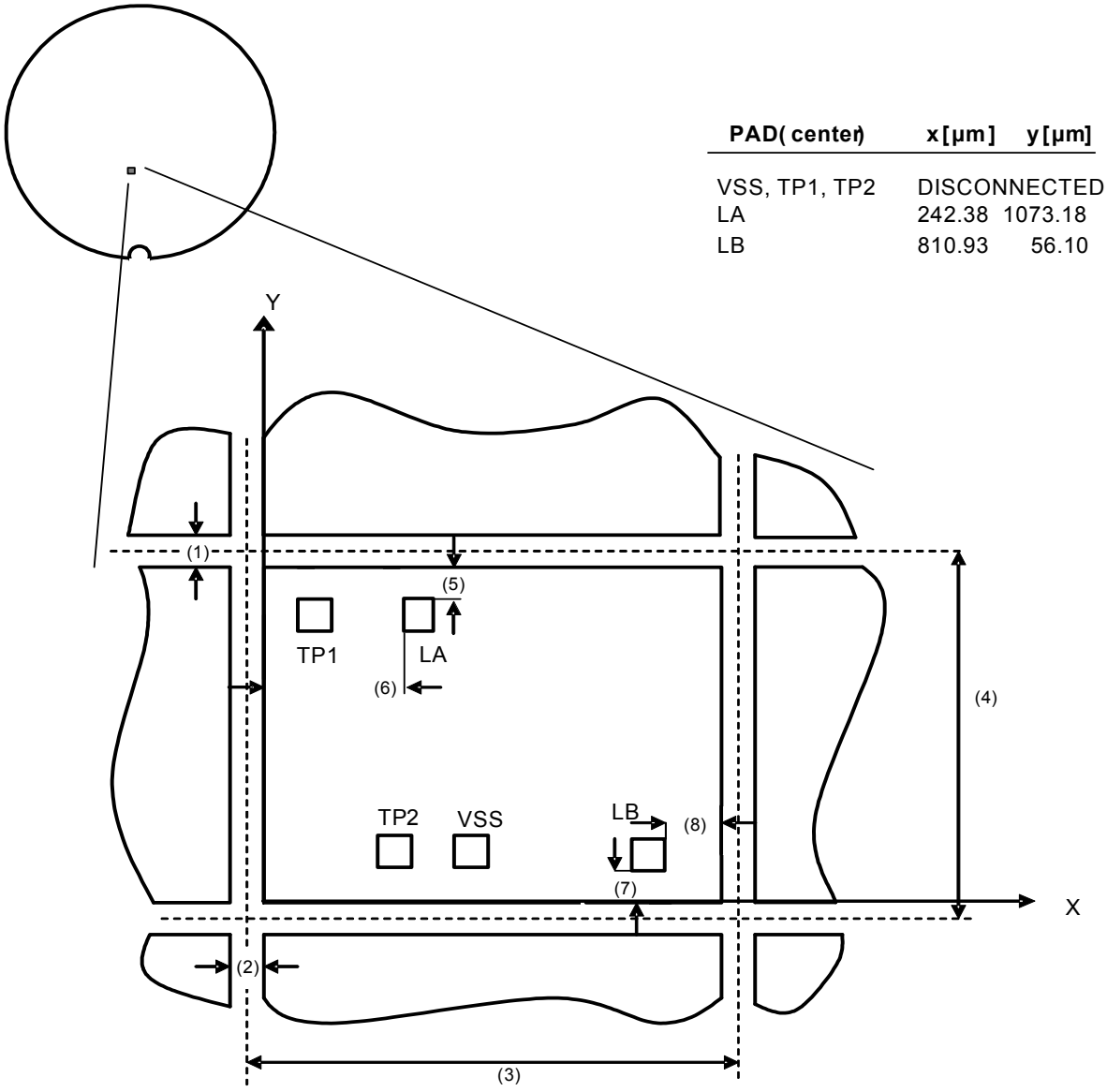
Remark: Substrate is connected to VSS.

7.6 Fail die identification

Electronic wafer mapping covers the electrical test results and additionally the results of mechanical/ visual inspection.

No inkdots are applied.

8. Chip orientation and bond pad locations



(1) X- Scribeline width :	Min: 5 µm; Typ: 15 µm	(5) LA bump edge to chip edge, y-length:	142.32 µm
(2) Y- Scribeline width :	Min: 5 µm; Typ: 15 µm	(6) LA bump edge to chip edge, x-length:	207.88 µm
(3) Chip step, x-length :	1216 µm	(7) LB bump edge to chip edge, y-length:	21.60 µm
(4) Chip step, y-length :	1265 µm	(8) LB bump edge to chip edge, x-length:	355.57 µm

(1) Lower left corner of metal sealring (X,Y) = 0,0

Fig 3. Chip orientation and bond pad locations

9. Functional description

9.1 Memory organization

The 4 kB EEPROM memory (MF1PLUS80) is organized in 32 sectors with 4 blocks and in 8 sectors with 16 blocks. The 2kB EEPROM memory (MF1PLUS60) is organized in 32 sectors with 4 blocks. One block consists of 16 bytes.

		Byte numbers within a block															
Sector	Block	0	1	2	3	4	5 (1)	6	7	8	9	10	11	12	13	14	15	Description
39	15	CRYPTO1 Key A						Access bytes				CRYPTO1 Key B or Data						Sector trailer 39
	14																	Data
	13																	Data
	...																	...
	...																	...
	2																	Data
	1																	Data
	0																	Data
	...																	...
	...																	...
	...																	...
32	15	CRYPTO1 Key A						Access bytes				CRYPTO1 Key B or Data						Sector trailer 32
	14																	Data
	13																	Data
	...																	...
	...																	...
	2																	Data
	1																	Data
	0																	Data
31	3	CRYPTO1 Key A						Access bytes				CRYPTO1 Key B or Data						Sector trailer 31
	2																	Data
	1																	Data
	0																	Data
	...																	...
	...																	...
	...																	...
0	3	CRYPTO1 Key A						Access bytes				CRYPTO1 Key B or Data						Sector trailer 0
	2																	Data
	1																	Data
	0																	Manufacturer data

(1) CRYPTO1 Key A in security level 0, 1, 2
Plaintext access byte in security level 3 (see Figure 6)

Fig 4. Memory organization

9.1.1 Manufacturer block

This is the first data block (block 0) of the first sector (sector 0). It contains the PICC manufacturer data. Due to security and system requirements this block is write protected after having been programmed by the PICC manufacturer at production.

9.1.2 Data blocks

Sectors 0 to 31 contain 3 blocks each and sectors 32 to 39 contain 15 blocks each for data storage.

The data blocks can be configured by the access bits as

- read/write blocks for storing binary data
- value blocks (e.g. counters, where additional commands like increment and decrement for direct control of the stored value are provided)

An authentication command must be carried out before any operation to allow for further commands.

9.1.2.1 Value blocks

The value blocks allow counter functions (valid commands: read, write, increment, decrement, restore, transfer).They have a fixed data format that permits error detection and correction with backup management. A value block can only be generated through a write or transfer operation of the following format:

- Value: Signifies a signed 4-byte value. The lowest significant byte of a value is stored in the lowest address byte. Negative values are stored in standard 2´s complement format. For reasons of data integrity and security, a value is stored three times, twice non-inverted and once inverted.
- Adr: Signifies a 1-byte address, which can be used to save the storage address of a block. The address byte is stored four times, twice inverted and non-inverted. During increment, decrement, restore operations the address (block number) remains unchanged. The address byte within the transfer command can be changed if the command is done to another block then from then from which increment/decrement/restore were performed.

The idea is to store the value in two blocks. Prior to incrementing/decrementing, the consistency of the blocks are checked. If one is corrupted, it shall be updated by the value of the other block. If the value is different, it can be decided if the higher or lower value shall be written to both blocks. It is done in the following steps:

- Store the value in two blocks (block A and block B) according to the format described in Figure 5
- Increment/Decrement block A
- Transfer the value (send the result) to block B
- Restore (Copy) the value from block B to block A

For performance reasons security level 3 offers also combined increment/decrement operation with restore/transfer operation, see Section 9.7.5.

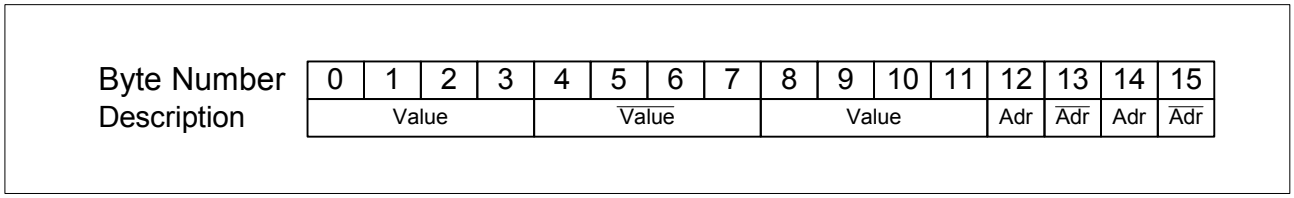


Fig 5. Value blocks

9.1.3 Sector trailer

Each sector has a sector trailer in the last block.This sector trailer is located in block 3 of each sector in the first two kB (sector 0 to sector 31) of the NV-memory and in block 15 of each sector in the upper 2 kB (sector 31 to sector 39) of the 4 kB NV-memory.

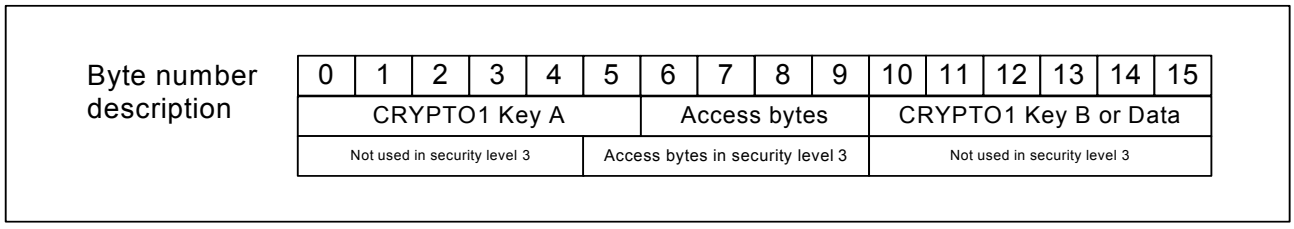


Fig 6. Sector trailer

Each sector trailer holds:

- secret keys A and B (optional, can be also data),
- access conditions for the four blocks or respective sixteen blocks of that sector, which are stored in bytes 6...9. The access bits also specify the type (read/write or value) of the data blocks.
- byte 5 defines if plain communication can be used in security level 3 after the authentication. After the switch to security level 3, the global access condition for byte 5 is used out of the MFP configuration block (see Section 10.10). By updating the byte in the sector trailer, the access condition for plain communication are overwritten by the value in the sector trailer. For a L3 card, the value for this access byte is set per default to 0Fh (plain communication for all blocks, see Section 10.11) and can be changed in security level 0.

In security level 3 updating the sector trailer is secured with an anti tearing mechanism.

9.1.4 AES keys

AES keys are not shown in the memory map. The keys are stored on top of the other data and can be updated and used by referencing the so called Key Nr (see Table 111). In security level 3, anti tearing is supported for the update of AES keys as well as for the update of the sector trailer. In security level 2, anti tearing is supported only for the update of AES keys.This on-board anti tearing mechanism is done by the PICC itself. The EEPROM stays in a defined status, even if the PICC is brought out of the field during write operations.

9.1.5 Proximity Check

The security level 3 offers a proximity check method by a precise time measurement of a challenge-response interaction. It is described in detail in Section 9.7.6.

9.1.6 Multi sector authentication

In security level 2 and 3, multi sector authentication can be used to optimize the performance and minimize the number of authentications. The decision for whether or not multi sector authentication can be used operates as follows:

1. The card is authenticated for sectorX with a KeyM
2. The reader tries to write/read/perform value operation to another sectorY where KeyN is needed to get access.
3. If KeyM has the same value as KeyN, no additional authentication is needed. The reader can immediately read/write data from sectorY or perform value operations.

The PICC itself sees KeyM as the authentication key and not KeyN. As such it is possible to change KeyN without losing the authentication.

The type of key (Key A or Key B) needs to match. It is not mandatory that the sectors are subsequent, the sectors just need to be operated one after each other.

It is possible to configure a card in such a way that operating with only one authentication is needed in security level 3 to read/write out all memory. The same applies also for security level 2 authentications (one is AES based, one is CRYPTO1 based).

9.1.7 Originality function

The originality function is implemented by an AES authentication as described in Section 9.7.2.2 with the originality key (see Section 10.7). The authentication shall be performed in ISO 14443-4 protocol layer (see also Section 9.2.2).

9.2 Card activation and communication protocol

The ISO/IEC 14443-3A anticollision mechanism allows for simultaneous handling of multiple PICCs in the field. The anticollision algorithm selects each PICC individually and ensures that the execution of a transaction with a selected PICC is performed correctly without data corruption from other PICCs in the field.

There are two different versions of the PICC, one having a unique 7 byte serial number (UID), the other having a unique 4 byte serial number, programmed into a locked part of the NV-memory which is reserved for the manufacturer. Due to security and system requirements these bytes are write-protected after being programmed by the PICC manufacturer at production time. As such, the customer must decide which UID length to use when ordering the product.

9.2.1 Backwards compatibility protocol

The backwards compatibility of this product, as used in security level 1 and security level 2, must run on the same protocol layer as MIFARE 1K, 4K and Mini. The protocol is formed out of the following components:

- Frame definition:
  According to ISO/IEC 14443-3
- Bit coding:
  According to ISO/IEC 14443-2
- Error code handling:
  Handling is proprietary as error codes are formatted in half bytes. The used error codes (NACK - Not Acknowledge) are described in Section 10.8
- Command specification:

  Commands are proprietary. Please use the specification as in Ref. 1, Ref. 2 and Ref. 3 and the additional commands, which are only implemented in MIFARE Plus as described in this data sheet.

The following security levels can be run on this protocol:

- Security Level 0
- Security Level 1
- Security Level 2

9.2.2 ISO/IEC 14443-4 Protocol

The ISO/IEC 14443-4 Protocol (also known as T=CL) is used in many processor cards. For MIFARE Plus this protocol is used in the following security levels:

- Security Level 0
- Security Level 1- only for the security level switch.
- Security Level 2 - only for updating AES Keys and configuration blocks as well as for the security level switch.
- Security Level 3
  During personalization, the PICC can be configured to support RandomID in security level 3. The user may decide whether Random ID or fixed UID shall be used and configure this in the field configuration block (see Section 10.9). According to ISO/IEC 14443-3 the first anticollision loop, see MIFARE application note ISO/IEC 14443 PICC Selection, will return the Random Number Tag 0x08, the 3 bytes Random Number and the BC, if Random ID is used.

  The retrieval of the real UID in this case can be done using the Virtual Card Select Last command, as described in Section 9.7.7 or by reading out block 0.

9.3 Migration concept

There are four security levels of the product:

- Security level 0:
  Initial delivery configuration
- Security level 1:
  Functional backwards compatibility mode (with MIFARE 1K/4K/Mini) with an optional AES authentication.
- Security level 2:
  3 Pass Authentication based on AES followed by MIFARE CRYPTO1 authentication, communication secured by MIFARE CRYPTO1
- Security level 3:
  3 Pass Authentication based on AES, new data manipulation commands secured by encryption and MAC-ing method, using AES.

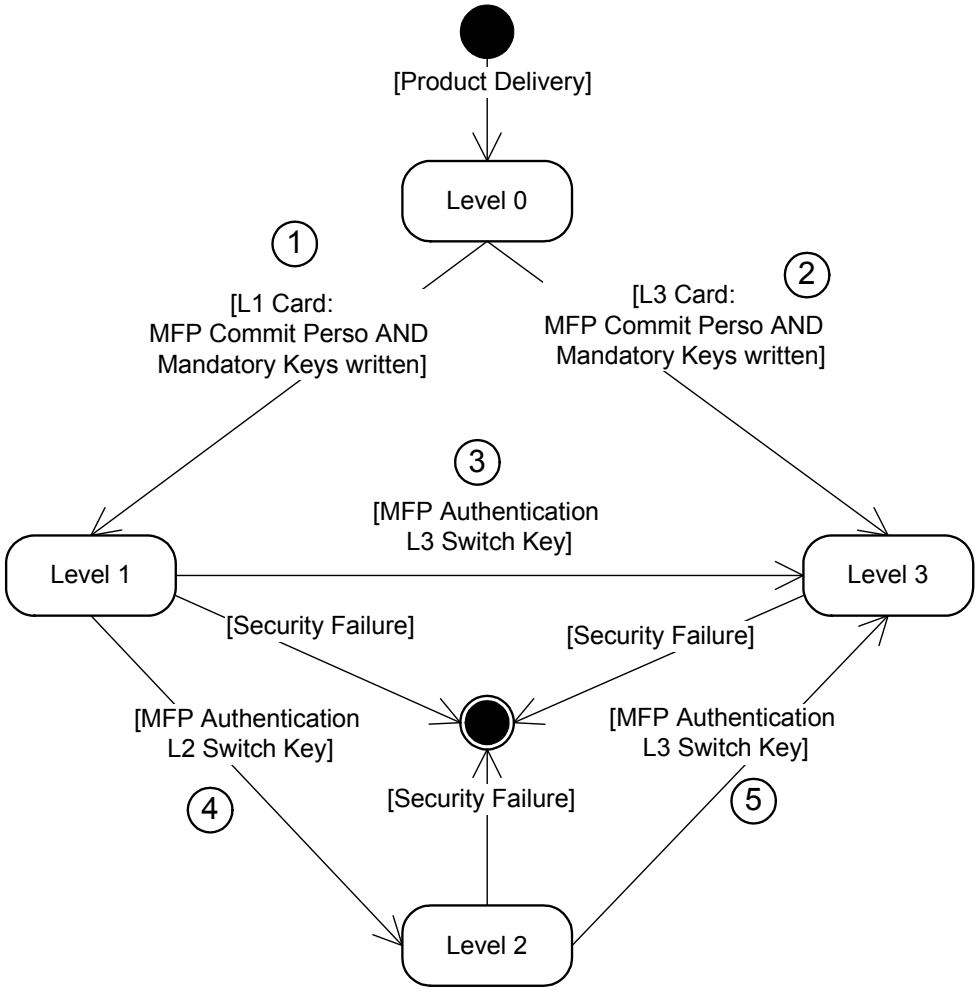


Fig 7. Migration Concept MIFARE Plus

Figure 7 shows the possible migration concept of MF1PLUSx0y1:

1. The product is delivered in security level 0. Depending on the order code, the selected product is a ’L1 card’ or a ’L3 card’. If it is a ’L1 card’, the PICC will switch after all mandatory keys are written to security level 1.
2. If it is a ’L3 card’, the PICC will switch after all mandatory keys are written directly to security level 3.
3. The ’L1 card’ in security level 1 can be switched after an authentication with the L3 switch key to security level 3.
4. The ’L1 card’ in security level 1 can be switched after an authentication with the L2 switch key to security level 2.
5. The ’L1 card’ in security level 2 can be switched after an authentication with the L3 switch key to security level 3.

9.4 Security level 0

Security level 0 is the initial delivery configuration of the PICC. The card activation as well as the protocol can be performed in one of the following two ways:

- Backwards compatibility protocol as described in Section 9.2.1
- ISO/IEC 14443-4

Depending on the chosen protocol layer, the commands described in the following sections are integrated into the specific protocol. In this level only the originality function and updating of the AES keys as well as any data is possible.

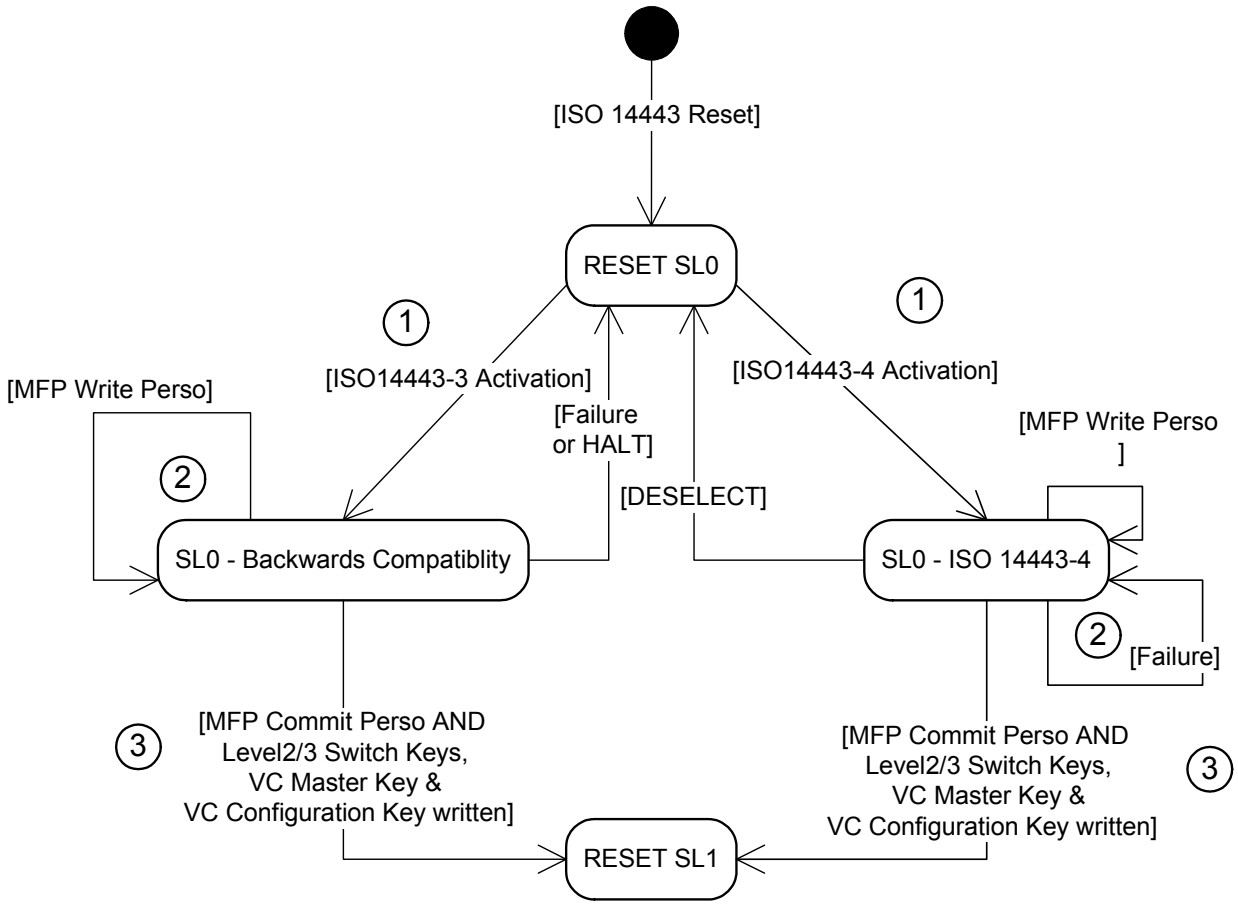


Fig 8. Security Level 0 State Diagram

1. The card can be activated to the backwards compatibility mode and to ISO 14443-4 layer.
2. All blocks and keys can be written in plain. The mandatory keys need to be updated to successfully send the Commit Perso command.
3. If the mandatory keys are written, one can successfully switch to security level 1, by sending the commit perso command.
4. A reset and a new card activation is needed to activate the security level 1.

The following keys need to be written using ’Write Perso’ (see Section 9.4.1) before the PICC can be switched to security level 1 using the command ’Commit Perso’ (see Section 9.4.2):

- Card Configuration Key
- Card master Key
- Level 2 switch Key
- Level 3 switch Key

It is also highly recommended to change all sector AES keys as well as the data within this security level in a secure environment.

It is possible to use the originalty function to find out, if the product is produced by NXP or not.

If the card is a ’L3 card’ the commit perso will switch the card directly to security level 3 instead of the security level 1. For a ’L3 card’, only the Card Configuration Key and the Card master Key need to be changed. Also here a reset and new card activation is needed to directly act in the new security level.

9.4.1 Write Perso

This command is used to change the data and AES keys from the initial delivery configuration to a customer specific value. The communication is in plain.

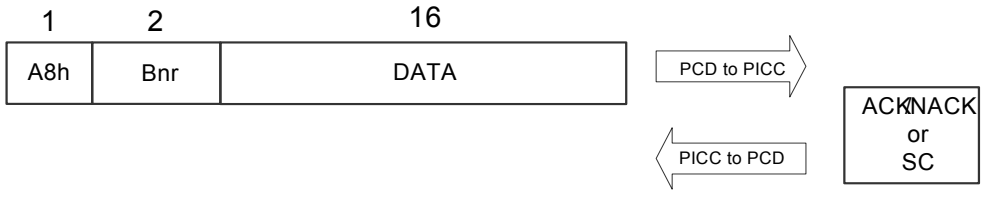


Fig 9. Write Perso

Table 3. Message description Write Perso

Name	Length	Description	Value
Command Code	01h	Command Code of Write Perso	A8h
BNr	02h	Block or Key to be written to	see Table 111 or see Figure 4
Data	10h	Value of the key or data, which shall be written (in plain)	

Table 4. Response description Write Perso

Name	Length	Description	Value
ACK/NACK or SC		Status Code from the PICC for ISO/IEC 14443-4 (see Section 9.2.2) or Acknowledge/Not Acknowledge from the PICC for backwards compatibility protocol (see Section 9.2.1)	see Table 112

9.4.2 Commit Perso

This command is used to finalize the personalization and switch up to security level 1. The command will only answer with the Status Code or Acknowledge, if all mandatory keys were changed with the command Write Perso prior to sending this command. Immediately after sending the response the card needs to receive a REQ or WAKEUP command to come back into the ACTIVE state and procede in security level 1.

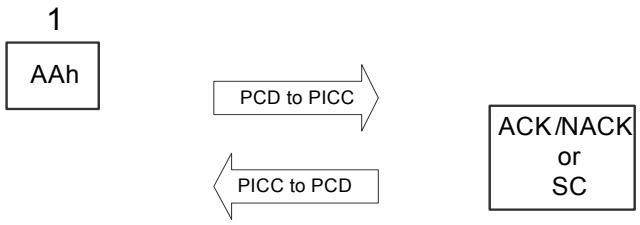


Fig 10. Commit Perso

Table 5. Message description Commit Perso

Name	Length	Description	Value
Command Code	01h	Command Code for Commit Perso	AAh

Table 6. Response description Commit Perso

Name	Length	Description	Value
ACK/NACK or SC		Status Code from the PICC for ISO/IEC 14443-4 (see Section 9.2.2) Acknowledge/Not Acknowledge from the PICC for backwards compatibility protocol (see Section 9.2.1)	see Table 112

9.5 Security level 1

In security level 1, the same functionality as in the MIFARE 1K/4K/Mini is available. Please find the specification in one of the following documents (see Ref. 1, Ref. 2 and Ref. 3). As such the protocol is also used in the same way as in the MIFARE 1K/4K/Mini (see Section 9.2.1).

Timings may differ to the MIFARE 1K/4K/Mini products.

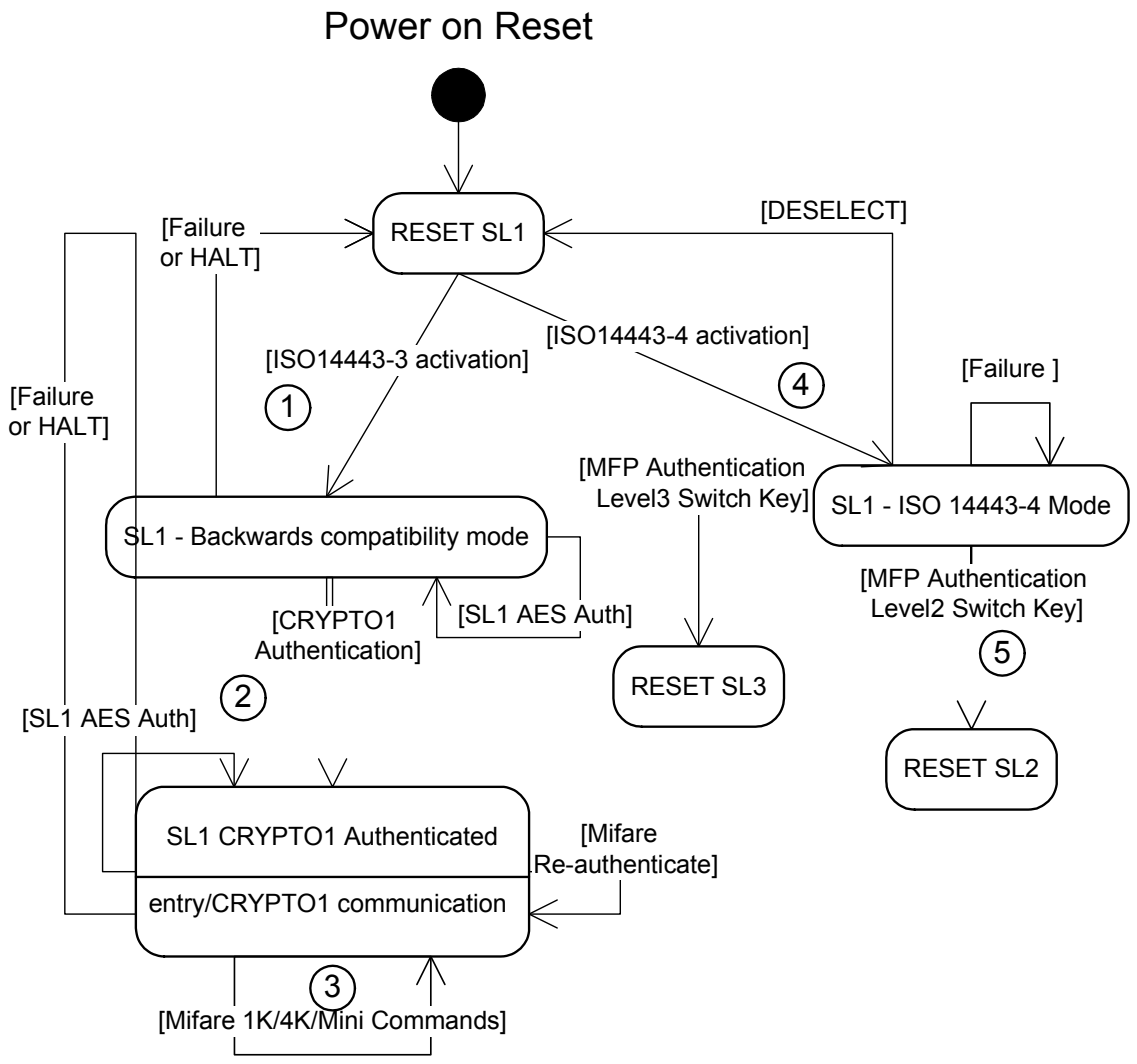


Fig 11. Security Level 1 State Diagram

1. An ISO 14443-3 activation is needed to come to the backwards compatible protocol (see Section 9.2.1). An authentication with the SL1 Card Authentication Key (see Table 111) as described in Section 9.6.1 is possible. This authentication is not combined with any session key within the transaction.

2. After a CRYPTO1 authentication as used in MIFARE 1K/4K/Mini, the PICC is authenticated with the CRYPTO1 key.
3. All commands as in MIFARE 1K/4K/Mini as well as one authentication with the SL1 Card Authentication Key (see Table 111) as described in Section 9.6.1 is possible. This authentication is not combined with any session key within the transaction.
4. A full card activation to ISO 14443-4 is needed to
5. authenticate with the SL2 switch key or the SL3 switch key. After authentication with SL2 switch key a reset and card activation is needed to start operating in the security level 2. The authentication can be done as described in Section 9.7.2.1 or Section 9.7.2.3. Please use the respective Key Nr as described in Section 10.7. After authentication with SL3 switch key a reset and card activation is needed to start operating in the security level 3.

It is possible to use the originalty function in this security level to find out, if the product is produced by NXP or not.

9.6 Security level 2

Security level 2 runs on the protocol as described in Section 9.2.1. The principal concept of the MIFARE products is that a sector can be authenticated with either Key A or Key B.

For security level 2, each sector contains:

- two AES Keys (128 bit) (Key A and Key B) (these keys are also used in security level 3)
- two CRYPTO1 Keys (48 bit) (Key A and Key B) (these keys are also used in security level 1)

The access conditions are set in the sector trailer as in MIFARE 1K/4K/Mini.

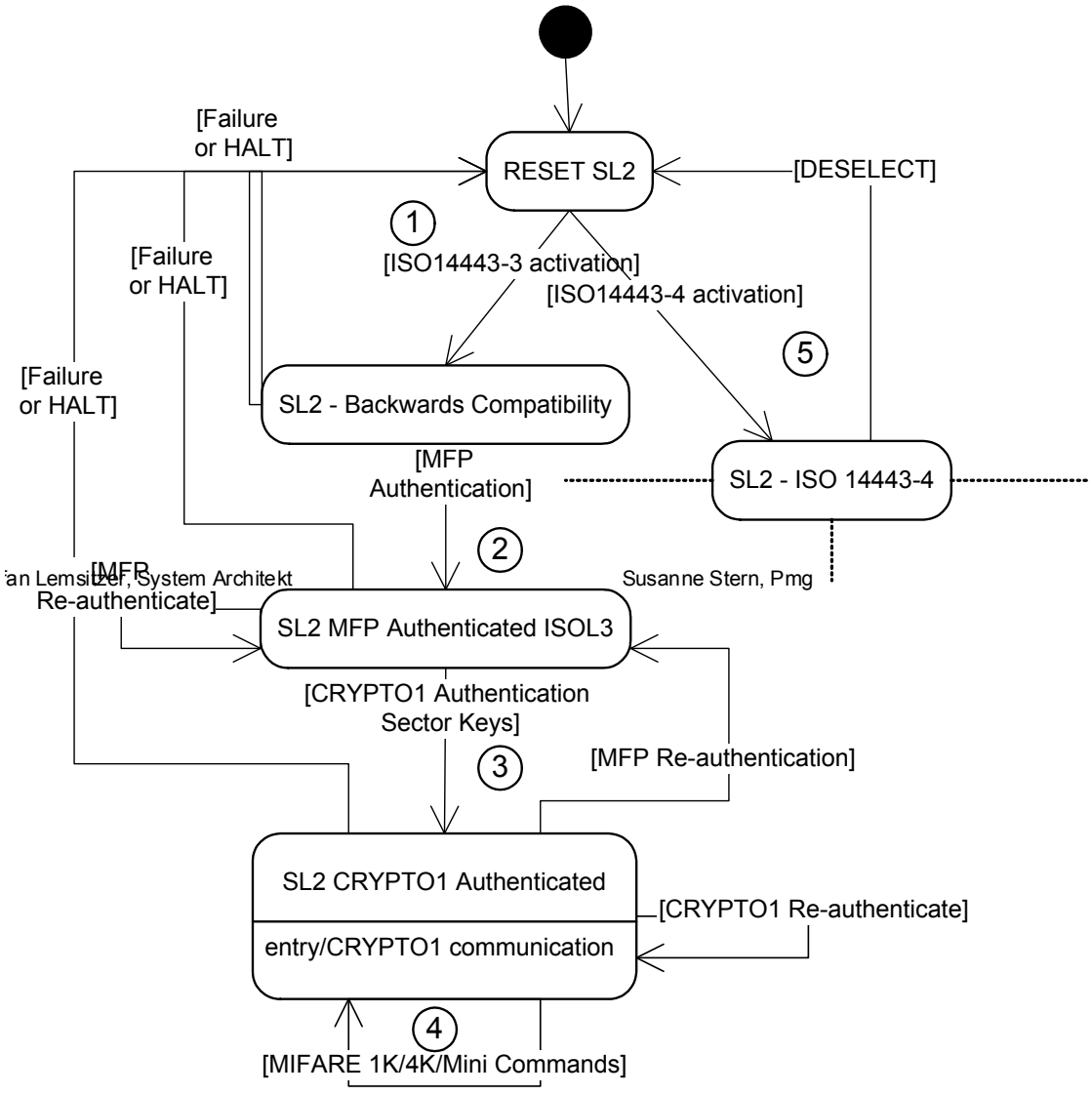


Fig 12. Security Level 2 State Diagram (1/2)

1. After activation according to ISO 14443-3 the PICC is in the backwards compatibility mode (see Section 9.2.1).
2. An authentication using AES is performed to generated a session key which is XORed with the CRYPTO1 key of the sector trailer.
3. The resulting key is used to authenticate with the CRYPTO1 algorithm.
4. The session key out of the CRYPTO1 authentication is used to secure the MIFARE 1K/4K/Mini commands using the CRYPTO1 communication protocol. In addition Multi Block Read (see Section 9.6.2) and Multi block Write (see Section 9.6.3) can be used.
5. Within this security level it is also possible to change the AES keys or to switch up to security level 3, this is described in Figure 13.

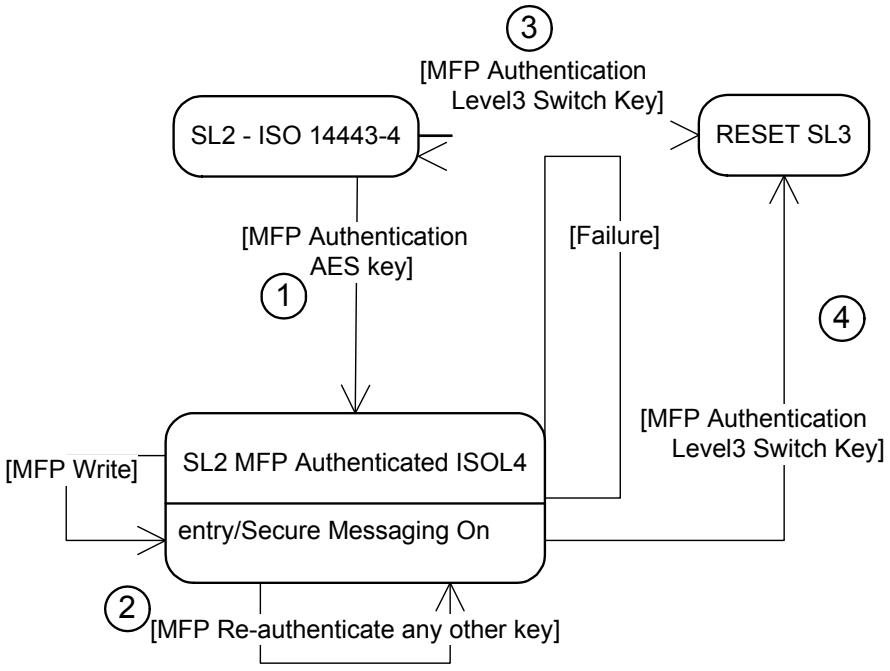


Fig 13. AES authentication in security level 2

1. After card activation until ISO 14443-4 and a AES authentication with the specified key, it is possible to
2. change AES keys in security level 2.It is possible to change the AES keys as well as configuration blocks (see Section 10.9 or Section 10.10) in this security level only in encrypted way. A full activation up to ISO/IEC 14443-4 layer is necessary before the same command set can be used to change the AES keys as described in Section 9.7.
3. After card activation until ISO 14443-4 it is also possible to switch to security level 3, if an AES authentication using Level 3 Switch Key is performed. The authentication can be done as described in Section 9.7.2.1 or Section 9.7.2.3, use the respective Key Nr as described in Section 10.7. A step back to a lower security level is not supported. A reset and a card activation is needed to operate in security level 3.

It is possible to use the originalty function in this security level if the product is produced by NXP or not.

9.6.1 Authentication in security level 2

Although the authentication is very similar to the one described in Section 9.7.2.3 there are some differences:

- The protocol used is described in Section 9.2.1.
- The session key is derived in a different way than in Section 9.7.2.
- The resulting value of the session key is XORed with the CRYPTO1 key in the sector trailer. The result is used to secure communications with CRYPTO1 Algorithm using the protocol and commands defined in Ref. 1, Ref. 2 and Ref. 3 as well as the commands Multi Block Read (see Section 9.6.2) and Multi Block Write (see Section 9.6.3).

Encryption of the data is performed using AES CBC mode (see Ref. 12). The initial init vector for this authentication is 00h.

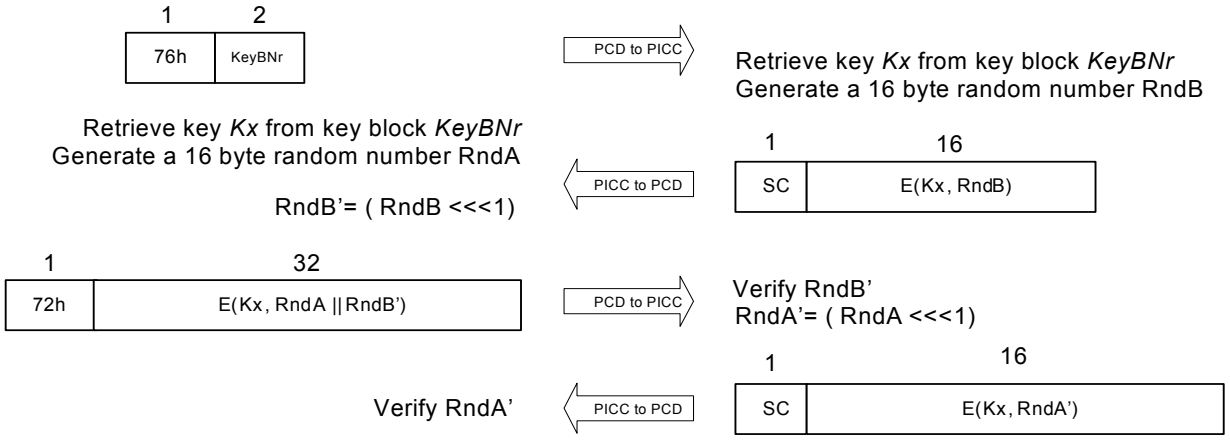


Fig 14. Authentication in security level 2

Table 7. Message description first step authentication in security level 2

Name	Length	Description	Value
Command Code	01h	Command Code of the first authentication	76h
KeyBNr	02h	Key Number of the key to be authenticated	see Table 111

Table 8. Answer description first step authentication in security level 2

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
E(Kx, RndB)	10h	Random number of PICC (RndB), encrypted using AES with the Key referenced over the KeyBNr (see Table 112)	

Table 9. Message description second step authentication in security level 2

Name	Length	Description	Value
Command Code	01h	Command Code of the second step within the authentication	72h
E(Kx, RndA || RndB')	20h	The random number of the reader (RndA) is concatenated with the modified random number of the PICC. The random number of the PICC is modified by a left rotation by 1 byte (RndB<<<1). The resulting 32 bytes are encrypted using AES with the Key referenced by the KeyBNr (see Table 112)	

Table 10. Response description second step authentication in security level 2

Name	Length	Description	Value
SC	01h	Success or Error Code from the PICC	see Table 112
E(Kx, RndA')	10h	Random number of reader (RndA) is modified by a left rotation of 1 byte (RndA<<<1) and encrypted using AES with the Key referenced via the KeyBNr (see Table 111)	

As a result one session key is generated using the following method:

1. Retrieve the following bit streams:
   a. A = RndA[b39...b00]
   b. B = RndB[b39...b00]
   c. C = RndA[b95...b56]
   d. D = RndB[b95...b56]
2. Perform an XOR-operation on value C and D to retrieve E. E = RndA[b95...b56] XOR RndB[b95...b56]
3. Concatenate the items in the following way:

   A || B || E || 33h
4. Encrypt the resulting data using AES CBC mode (see Ref. 12), where the init vector is set initially to 00h, with the authentication key:

   cryptogram = E(Kx, A || B || E || 33h)
5. Take the 6 most significant bytes of the cryptogram and XOR it with the respective MIFARE CRYPTO1 key
6. Use the resulting 'new' MIFARE CRYPTO1 key for the communication within this authentication.

9.6.2 Multi block read

This command is used for reading one to three blocks of one sector, which reduces the transaction time due to omitted protocol time.

This command is used together with the MIFARE CRYPTO1 protocol (see Ref. 1, Ref. 2 and Ref. 3). The framesize of the PCD must support the number of blocks to be read. For instance, if two blocks shall be read, the framesize must be equal to or greater than 32 bytes. If three blocks shall be read, the framesize must be equal to or greater than 48 bytes.

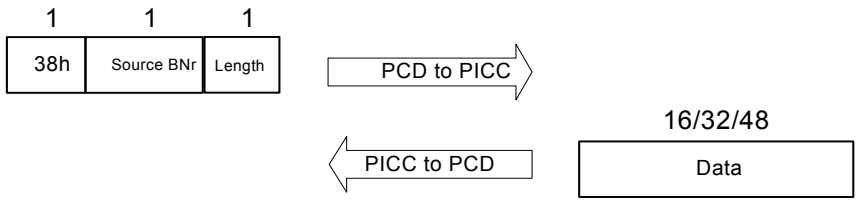


Fig 15. Multi block read

Table 11. Message description Multi Block Read

Name	Length	Description	Value
Command Code	01h	Command Code of the Multi Block Read	38h
Source Bnr.	01h	Block Number	Ref. 1, Ref. 2 and Ref. 3
Length	01h	The number of blocks to be read. For sector trailers only a length of 1 is accepted.	01h to 03h

Table 12. Answer description Multi Block Read

Name	Length	Description	Value
Data	10h or 20h or 30h	Data	

9.6.3 Multi block write

Writing up to three blocks within one command reduces transaction time due to omitted protocol time. It is only possible to write up to three blocks with one command within one sector.

This command is used together with the MIFARE CRYPTO1 protocol (see Ref. 1, Ref. 2 and Ref. 3). The framesize of the PCD must support the number of blocks to be written. As such if two blocks shall be written, the framesize must be equal to or greater than 32 bytes. If three blocks shall be written, the framesize must be equal to or greater than 48 bytes.

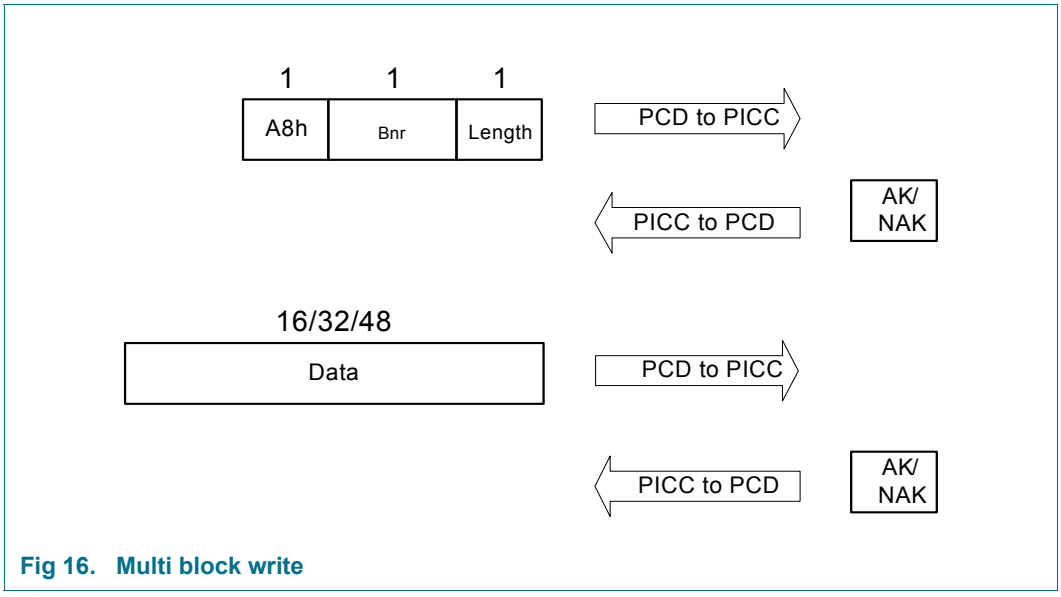


Fig 16. Multi block write

Table 13. Message description Multi Block Write

Name	Length	Description	Value
Command Code	01h	Command Code of Multi Block Write	A8h
Bnr.	01h	Block Number	see Ref. 1, Ref. 2 and Ref. 3
Length	01h	The number of blocks to be written. For sector trailers only a length of 1 is accepted.	01h to 03h

Table 14. Answer description Multi Block Write

Name	Length	Description	Value
Acknowledge	Halfbyte	Acknowledge (ACK) or Not Acknowledge (NACK)	see Table 112

Table 15. Message description Multi Block Write

Name	Length	Description	Value
Data	10h/20h/30h	Data to be written	

Table 16. Answer description Multi Block Write

Name	Length	Description	Value
Acknowledge	Halfbyte	Acknowledge (ACK) or Not Acknowledge (NACK)	see Table 112

9.7 Security level 3

Security level 3 operates on ISO/IEC 14443-4 protocol layer. The customer can use Random ID during card activation, see Section 9.2.2.

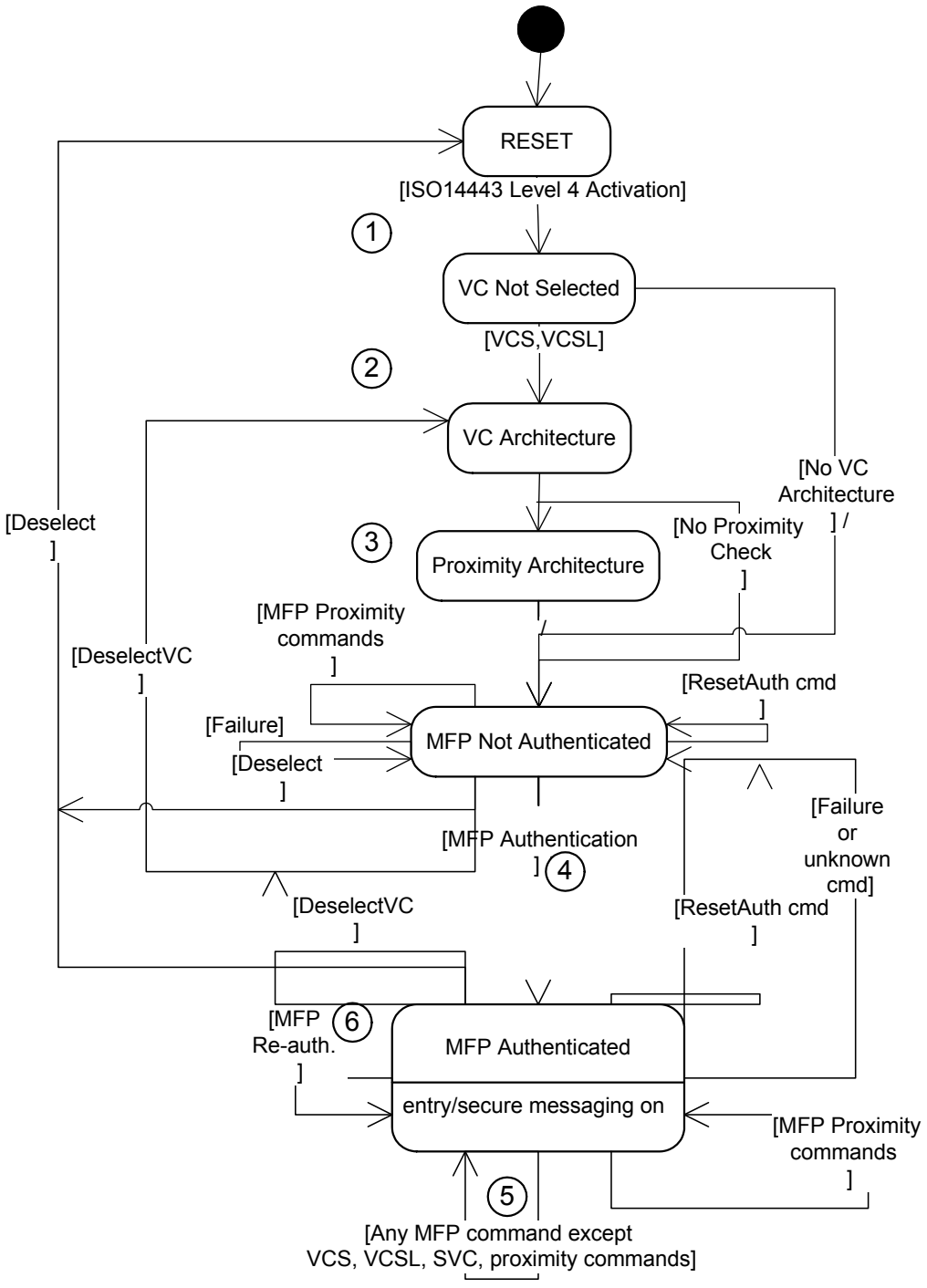


Fig 17. Security Level 3 State Diagram

1. An ISO 14443-4 activation is needed for security level 3.
2. The virtual card architecture can be carried as described in Section 9.7.7.
3. A proximity check is recommended to find out about relay attacks, see Section 9.7.6.
4. After the optional virtual card architecture and the proximity check the PICC is not authenticated. An AES authentication is needed for any PICC command except Proximity Check, Virtual Card and Authentication itself.
5. After an AES authentication all commands as described in Section 9.7.3 to Section 9.7.5.
6. An operation on a sector with a different AES key or confguration block needs a Re-authentication.

In security level 3, an AES authentication between PICC and reader is conducted, where two keys are generated as a function of the random numbers of the PICC as well as the reader and the shared key. These two unpredictable keys are exclusively used to secure the data, which is exchanged on the interface between the card and reader. One of the two keys is used to ensure the confidentiality of the command while the other key ensures the integrity of the command.

The reader can decide which security needs to be used in the communication between PICC and reader. In the simplest case, all commands carry a MAC, such that the PICC will only accept commands from the reader with which it has authenticated. Tampering of operands and messages is detected by checking the MAC. Also all responses contain a MAC, so that the reader on each response knows that neither the command nor the response has been tampered with.

If performance is of highest priority, the card can be configured to allow MACs on the Read commands to be omitted. The card will then accept read commands without knowing whether they are genuine. However, there is a mechanism by which the reader can still determine whether or not the read response was resulting from the unmodified Read command that it sent.

Other commands, like Write-commands, are always MACed, such that no card modifying operation may be carried out without the card having assured that the command is genuine.

For each command, the reader can decide whether or not to request that a MAC be included on the response. When the appropriate MAC is received, due to linking of MACs (see Section 9.7.1.3) the reader knows that the command and all commands before it were properly executed.

Finally, if performance matters more than confidentiality, or if the application encrypts the data with another key, each data block in a sector can be configured to allow or disallow sending/receiving data in plain.

9.7.1 Security concept level 3

A MIFARE Plus transaction includes a set of operations from card activation, authentication to the reading and changing of data on the card. Each interaction with data on the card requires an authentication with the appropriate sector key. The result of such an authentication is called a session. A **transaction** can be a composite of several **sessions**, which always begin with a first authentication and finish with the start of the next first authentication or may end with an error code. In between there may be several sessions with following authentications. In one session two session keys are generated to ensure the confidentiality and integrity of the data that is exchanged.

9.7.1.1 Authenticity

Authentication is the act of establishing or confirming something (or someone) as genuine. MIFARE Plus offers two different authentications:

- First Authentication (see Section 9.7.2.1)

- Following Authentication (see Section 9.7.2.3)

Both authentications are performed using AES (see Ref. 12) and generate two session keys, which will be used for the confidentiality and integrity of commands within a session.

The first authentication involves the following items of:

A Transaction Identifier (TI) must be used to cryptographically bind together all messages within one transaction. The TI is defined by the card and sent back with the first authentication.

The transaction identifier is used within the init vector for all encryptions. As such the init vector for the first authentication is 00h. For the following authentication it is the Transaction Identifier from the previous first authentication and the counter set to 00h (see Figure 18).

The PCD and PICC capabilities are exchanged between the PICC and PCD.

After any first authentication the read and write counters (R_Ctr, W_Ctr) are reset to 00h.

It is possible to reset the authentication using the command ResetAuthentication (see Section 9.7.2.3).

9.7.1.2 Confidentiality

The confidentiality of communication is assured by the encryption performed using AES CBC mode (see Ref. 12). Where it is required prior to CBC-encryption, the command is padded to a multiple of 128 bits in length by appending a single 80h and 00h (single or multiple) (see ISO/IEC 9797 section 2, padding method 2).

The init vector of all encryptions on command (typically write commands, but also the command sent during following authenticate) is formed out of the Transaction Identifier, which is sent by the PICC within the first authentication as well as the value of the read and write counters (R_Ctr, W_Ctr) (see Figure 18).

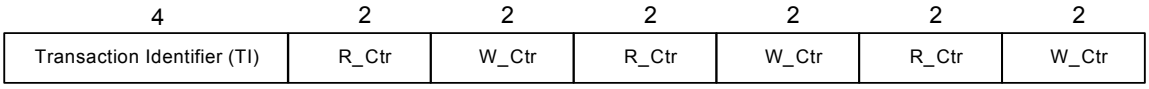


Fig 18. Initialization vector (IV) for encryption on command

The init vector of all encryptions on responses (typically read commands, but also the responses during the following authenticate) is formed out of the Transaction Identifier (TI), which is sent by the PICC within the first authentication as well as the value of the read and write counters (R_Ctr, W_Ctr) (see Figure 19).

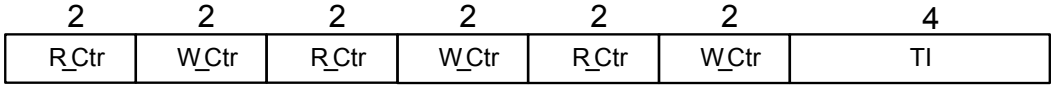


Fig 19. Initialization vector (IV) for encryption on Response

9.7.1.3 Integrity

Integrity is ensured by the calculation of MACs (Message Authentication Codes). These MACs are calculated using AES as the underlying block cipher, according to the CMAC standard described in NIST Special Publication 800-38B, and are truncated to 8 bytes by the following method: The concatenation of **every second byte starting from the second MSB** form the MAC.

Padding is performed by appending a single 80h and multipe 00h (see ISO/IEC 9797 section 2, padding method 2).

Padding and the initialization vector (before every command 00h) are also applied according to this standard. Each MAC is computed on data as indicated in the diagram of each command.

Integrity on Write command and value operations:

Each Write command as well as Increment/Decrement/Restore/Transfer commands are counted. The counter (called W_Ctr) is included in the MAC that is calculated over the command. The representation of the counter is formatted as defined in the Little-Endian standard (the least significant byte is represented first). Both the reader as well as the cards are counting such that the actual value of the W_Ctr never needs to be transmitted. The W_Ctr is reset to 00 00h after the first authentication within the transaction. A command using W_Ctr in its MAC and requesting for a MAC on a response is handled as follows. If W_Ctr = n at the moment the application wants to send the command, the MAC on the command is calculated including W_Ctr = n. The MAC on the response will be calculated over a value n + 1. The W_Ctr is included in the MAC calculation as well as in the init vector for the encryption. It is recommended to follow this sequence:

1. Encrypt the data, which shall be sent to the PICC, if encryption shall be used.
2. Calculate the MAC.
3. Increment the W_Ctr

4. Dispatch the command to the PICC.
5. Receive the response from the PICC.
6. Verify the response and check the MAC (if applicable)

Depending on the chosen command, either a MAC on the command or on the response can be applied. The MAC on the command is calculated in the following way:

1. Concatenate the following items:
   Command Code || W_Ctr || Transaction Identifier (TI) || Block Number || Data || Optional Padding
   if the payload is encrypted, then the data is encrypted. If the payload is in plain, then the data is in plain. Vor value operations, it may apply that both source block number after destination block number need to be concatenated instead of the block number.
2. Calculate a MAC according to Ref. 13 the init vector for the AES encryption is 00h
3. Truncate to 8 byte stream as indicated in the first paragraph of this section.
4. Attach to the command.

The MAC on the response is calculated in the following way:

1. Concatenate the following items:
   Status Code || W_Ctr || Transaction Identifier (TI) || Padding
2. Calculate a MAC according to Ref. 13 the init vector for the AES encryption is 00h.
3. Truncate to 8 byte stream as indicated in the first paragraph of this section.
4. Attach to the response.

Integrity on Read commands:

All Read commands sent by the PICC are counted with a read counter (R_Ctr). The representation of the counter is formatted as defined in Little-Endian (the least significant byte is represented first). The counter is included in the MAC that is calculated over the response or command. Both sides count responses such that the actual value of the R_Ctr never needs to be transmitted. The R_Ctr is reset to 00 00h after the first successful authentication. The R_Ctr is included in the MAC calculation as well as in the init vector for the encryption of the communication (see Section 9.7.1.2). It is recommended to follow this sequence:

1. Calculate the MAC (if applicable).
2. Increment the R_Ctr
3. Dispatch the command to the PICC.
4. Receive the response from the PICC.
5. Verify the response and check the MAC (if applicable)
6. Decrypt the data.(if applicable)

Depending on the chosen command, either a MAC on the command and/or on the response can be applied. The MAC on the command is calculated in the following way:

1. Concatenate the following items:
   Command Code || R_Ctr || Transaction Identifier (TI) || Block Number || Ext || Padding
2. Calculate a MAC according to Ref. 13 the init vector for the AES encryption is 00h.

3. Truncate to 8 byte stream as indicated in the first paragraph of this section.
4. Attach to the command.

If no MAC on the response is used, a **session read counter** counts the number of unmaced read commands and is automatically reset, if:

- a new authentication was successfully performed
- a MAC on the read command was sent to the PICC.

It is possible to define the maximum number of unmaced read commands and therefore the limit of the session read counter, by configuration in the MFP configuration block (see Section 10.10).

The MAC on the response is calculated in the following way:

1. Status Code || R_Ctr || Transaction Identifier (TI) || BNr of first response || Ext of first response || Payload (encrypted or plain) || Padding.
2. If the last command did not include the MAC, the MAC includes the data of the last command (as indicated in step 1) and in addition || BNr_2 || Ext_2 || $Data_2$
3. The data is concatenated until a MAC was requested. The sequence is after this MAC calculation (according to Ref. 13) cleared.
4. Truncate to 8 byte stream as indicated in the first paragraph of this section.
5. Attach to the response.

9.7.1.4 Other security features

A proximity check (see Section 9.7.6) can be performed to verify if the PICC is within the proximity of the PCD.

The usage of Random ID is recommended to provide privacy to the end user. The retrieval of the UID can be done as described in Section 9.7.7.

9.7.2 Authentication

9.7.2.1 First authentication

The first authentication starts when the PCD sends a 'First Authenticate' command, indicating the key to authenticate with. This is either a key A or B of a specific sector or it is a special key. The parameter must be filled with the appropriate key number (see Table 111).

The authentication in general is described in Section 9.7.1.1.

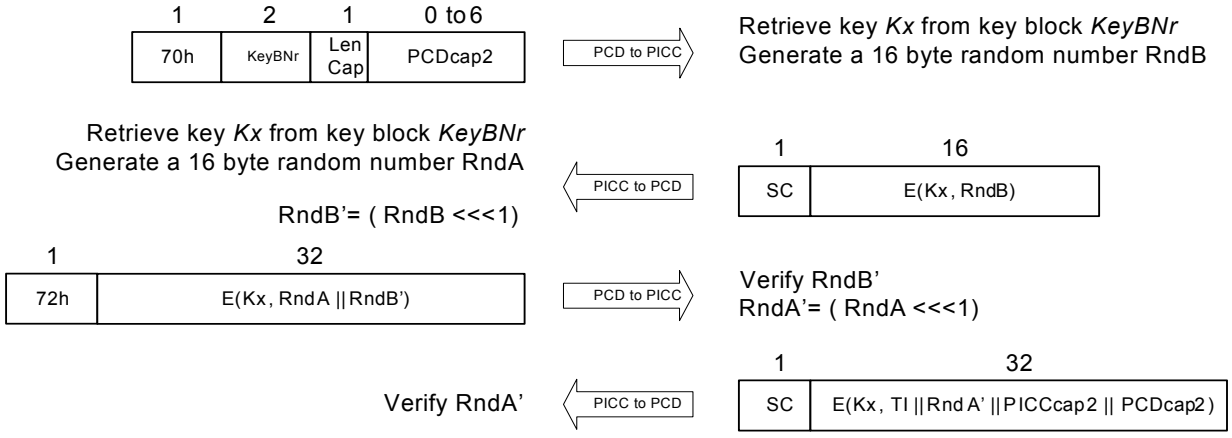


Fig 20. First authentication

Table 17. Message description first authentication

Name	Length	Description	Value
Command Code	01h	Command Code of the first authentication	70h
KeyBNr	02h	Key Number of the key to be authenticated	see Table 111
LenCap	01h	Length of the capabilities to be sent in next parameter	00h to 06h
PCDcap2	00h to 06h	The capabilities of the PCD, which define what is the PCD capable to do. Any value can be used upon the requirements of the PCD.	

Table 18. Response first authentication

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
E(Kx, RndB)	10h	Random number of PICC(RndB), encrypted using AES with the Key referenced by the KeyBNr (see Table 111)	

Table 19. Message description second step within first authentication

Name	Length	Description	Value
Command Code	01h	Command Code of the second step within the authentication	72h
E(Kx, Rnd A ||Rnd B')			
	10h	The concatenated data, as described in the following rows in the following way is encrypted with the Key referenced by the KeyBNr (see Table 111)	
Rnd A	08h	The random number of the PICC.	
Rnd B'	08h	The random number of the PCD, which is modified with a left rotation by 1 byte.	

Table 20. Response second step first authentication

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
E(Kx, TI || Rnd A' || PICCcap2 || PCDcap2)			
	20h	The data concatenated, as described in the following rows in the following way is encrypted with the Key referenced by the KeyBNr (see Table 111)	
TI	04h	The Transaction Identifier is a random number generated with the first transaction and used during the whole transaction.	
Rnd A	08h	The random number of the PCD.	
PICCcap2	06h	The capabilities of the PICC, where: Rightmost two bytes (PICCcap2.5 and PICCcap2.6) can be defined, by changing the field configuration block (see Table 113). It is e.g. possible to reflect a key version or similar in the capabilities. The leftmost four bytes (PICCcap2.1 to PICCcap 2.4) can only be defined by NXP, the default value is 00h.	
PCDcap2	06h	The capabilities of the reader PICC, exchanged with the first command (see Table 17)	

As a result, two session keys are generated. One session key, KENC, is generated to perform the encryption. The other, K_{MAC}, is generated to calculate the Message Authentication Codes (MAC). The session keys are generated by encryption of the exchanged random values with the key used during the authentication. The two session keys are generated in the following way:

1. Retrieve the following bit streams:
   a. A = RndA[b39...b00]
   b. B = RndB[b39...b00]
   c. C = RndA[b95...b56]
   d. D = RndB[b95...b56]
   e. E = RndA[b71...b32]
   f. F = RndB[b71...b32]
   g. G = RndA[b127...b88]
   h. H = RndB[b127...b88]
2. Perform an XOR-operation on C and D to retrieve value I.

   I = C XOR D = RndA[95...56] XOR RndB[95...56]

   As well perform an XOR-operation on value G and H to retrieve J.

J = G XOR H = RndA[127...88] XOR RndB[127...88]

3. Concatenate the items in the following way to the final session key bases:

   Session key base K_{ENC} = A || B || I || 11h

   Session key base K_{MAC} = E || F || J || 22h

4. Encrypt the session key bases with the authentication key to retrieve the session key:

   K_{ENC} = E(Kx, Session key base K_{ENC})

   K_{MAC} = E(Kx, Session key base K_{MAC})

In addition, the Transaction Identifier is defined by the PICC, which is used throughout the transaction to avoid interleaving sessions. The read and write counters are reset to 00h. The new init vector is formed out of the new exchanged Transaction Identifier and the read and write counters (00h). The capabilities of the reader and card are also exchanged (PCDcap2 and PICCcap2).The session read counter (see Section 9.7.1.3) is reset and transfer buffer is invalidated.

9.7.2.2 Following authentication

Every authentication after the first authentication starts when the PCD sends a 'Following Authentication' command, indicating the key to authenticate with. This is a key A or B of a specific sector or it is a special key. The parameter must be filled with the appropriate key number (see Table 111). It is also possible to always use only a 'First Authentication' command, and to exchange the Transaction Identifier as well as the Capabilities in every session. The read and write counters as well as the session read counter would then be reset after every authentication as well as the transfer buffer would be invalidated. Nevertheless using the 'Following Authentication' command is a countermeasure against interleaving sessions and saves protocol time.

There is a difference between the first authentication in a transaction and following ones. In the process described in this chapter, it is assumed that the capabilities and transaction identifier are already exchanged, therefore these parameters are not part of the authentication. With the following authentication, the read and write counters as well as the session read counter are not reset but the transfer buffer is invalidated.

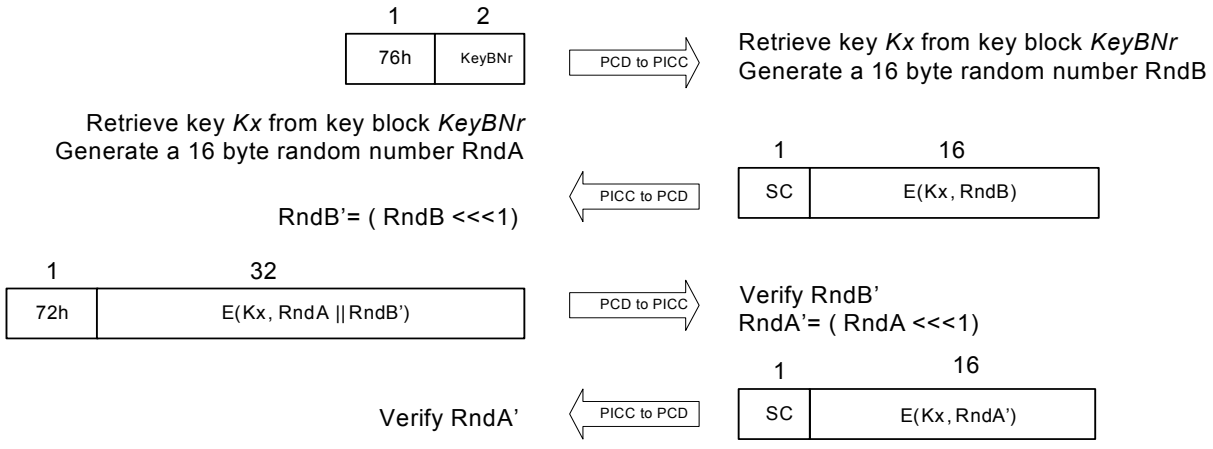


Fig 21. Following authentication

Table 21. Message description following authentication

Name	Length	Description	Value
Command Code	01h	Command Code of the following authentication	76h
KeyBNr	02h	Key Number of the key to be authenticated	see Table 111

Table 22. Response following authentication

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
E(Kx, RndB)	10h	Random number of PICC (RndB), encrypted using AES with the Key referenced over the KeyBNr (see Table 111). The init vector used is shown in Figure 19.	

Table 23. Message description second step within following authentication

Name	Length	Description	Value
Command Code	01h	Command Code of the second step within the authentication	72h
E(Kx, Rnd A || Rnd B')	20h	The random number of the reader (Rnd A) is concatenated with the modified random number of the PICC. The random number of the PICC is modified with a left rotation by 1 byte. The resulting 32 bytes are encrypted using AES with the Key referenced by the KeyBNr (see Table 111) The init vector for the encryption on this command is shown in Figure 18.	

Table 24. Response second step following authentication

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
E(Kx, RndA')	10h	Random number of PCD (RndA) is modified with a left rotation by 1 byte and gives RndA'. The result is encrypted using AES with the Key referenced over the KeyBNr (see Table 111). The init vector for the encryption on this response is shown in Figure 19.	

As a result, two session keys are generated. One session key, KENC, is generated to perform the encryption. The other, K_{MAC}, is generated to calculate to Message Authentication Codes (MAC). The session keys are generated by encryption of the exchanged random values with the key used in the conducted authentication. The two session keys are generated in the same way as described in Section 9.7.2.1.

9.7.2.3 Reset Authentication

This command is used to reset the authentication.

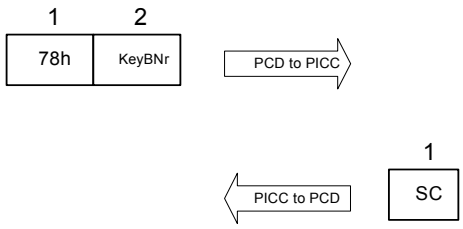


Fig 22. Reset authentication

Table 25. Message description reset authentication

Name	Length	Description	Value
Command Code	01h	Command Code of Reset Authentication	78h

Table 26. Response Reset authentication

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112

9.7.3 Read

The following options are available to the customer to chose from:

1. MAC on command data (command sent to the PICC)

   a) MAC on response from PICC

- Data in plain (not encrypted)
- Data encrypted

   b) No MAC on response from the PICC

- Data in plain
- Data encrypted

2. No MAC on command data

   a) MAC on response from PICC

- Data in plain
- Data encrypted

   b) No MAC on response from PICC

- Data in plain
- Data encrypted

The following table gives an overview of the options and the resulting command code.

MAC on command	Plaintext	MAC on response	Command Code Read
Yes	No	No	30h
Yes	No	Yes	31h
Yes	Yes	No	32h
Yes	Yes	Yes	33h
No	No	No	34h
No	No	Yes	35h
No	Yes	No	36h
No	Yes	Yes	37h

9.7.3.1 Read encrypted, no MAC on response, MAC on command

This command offers the possibility to read the data from one or multiple blocks in an encrypted way. A MAC is only used on the command sent to the PICC, no MAC is attached on the response. For information on the confidentiality, please refer to Section 9.7.1.2. For information on the integrity, please refer to Section 9.7.1.3.

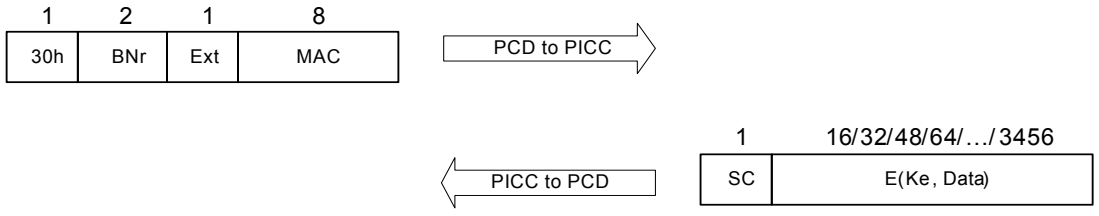


Fig 23. Read encrypted, No MAC on response, MAC on command

Table 27. Message description Read encrypted, no MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of the read encrypted, No MAC on response, MAC on command	30h
BNr	02h	Block Number of the first block to be read	see Table 111
Ext	01h	Number of blocks to be read	Sector Trailers do not count if Ext > 1.
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

The read counter (R_Ctr) is incremented just prior to dispatch of the command.

Table 28. Response Read encrypted, no MAC on response, MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
E(Ke, Data)	Multiple of 10h	The data to be read is encrypted with the session key as generated in the last authentication (see Section 9.7.2.1 or Section 9.7.2.3)	

9.7.3.2 Read encrypted, MAC on response, MAC on command

This command offers the possibility to read the data from one or multiple blocks in an encrypted way. A MAC is used on the command sent to the PICC and on the response received. For information on the confidentiality, please refer to Section 9.7.1.2, for information on the integrity, please refer to Section 9.7.1.3.

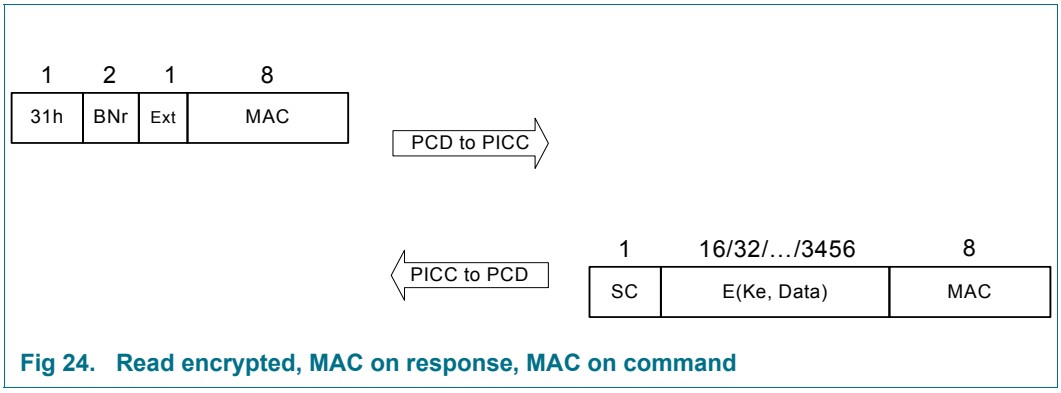


Fig 24. Read encrypted, MAC on response, MAC on command

Table 29. Command description Read encrypted, MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of the read encrypted, MAC on response, MAC on command	31h
BNr	02h	Block Number of the first block to be read	see Table 111
Ext	01h	Number of blocks to be read	Sector Trailers do not count if Ext > 1.
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

Table 30. Response Read encrypted, MAC on response, MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
E(Ke, Data)	Multiple of 10h	The data to be read is encrypted with the session key as generated in the last authentication (see Section 9.7.2.1 or Section 9.7.2.3).	
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

9.7.3.3 Read in plain, no MAC on response, MAC on command

This command offers the possibility to read the data in plain from one or multiple blocks. A MAC is used on the command and not on the response.

For information on the confidentiality, please refer to Section 9.7.1.2, for information on the integrity, please refer to Section 9.7.1.3.

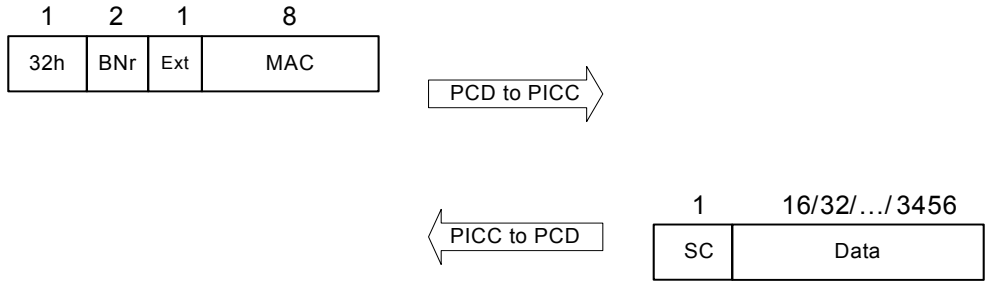


Fig 25. Read in plain, no MAC on response, MAC on command

Table 31. Command description Read in plain, no MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of the read in plain, no MAC on response, MAC on command	32h
BNr	02h	Block Number of the first block to be read	see Table 111
Ext	01h	Number of blocks to be read	Sector Trailers do not count if Ext > 1.
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

Table 32. Response Read in plain, no MAC on response, MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
Data	Multiple of 10h	The data to be read	

9.7.3.4 Read in plain, MAC on response, MAC on command

This command offers the possibility to read the data in plain from one or multiple blocks. A MAC is used on the command and the response. For information on the confidentiality, please refer to Section 9.7.1.2, for information on the integrity, please refer to Section 9.7.1.3.

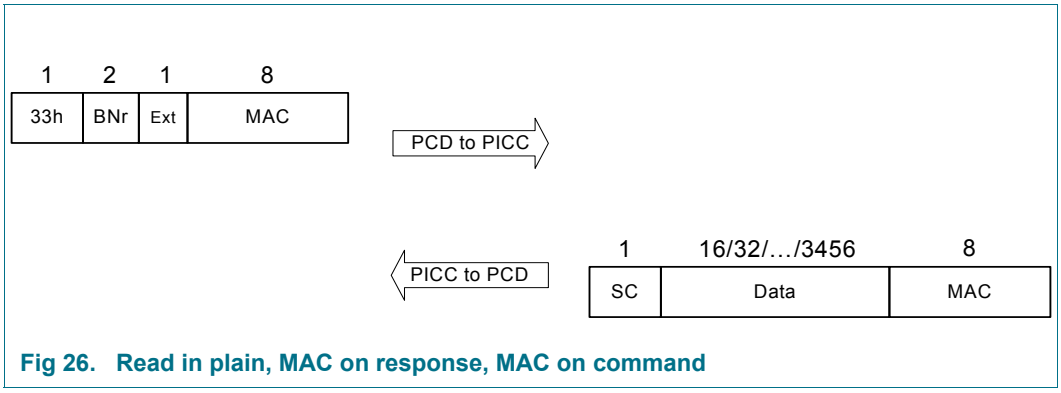


Fig 26. Read in plain, MAC on response, MAC on command

Table 33. Command description Read in plain, MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of the read in plain, MAC on response, MAC on command	33h
BNr	02h	Block Number of the first block to be read	see Table 114
Ext	01h	Number of blocks to be read	Sector Trailers do not count if Ext > 1.
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

Table 34. Response Read in plain, MAC on response, MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
Data	Multiple of 10h	The data to be read	
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

9.7.3.5 Read encrypted, no MAC on response, no MAC on command

This command offers the possibility to read the data from one or multiple blocks in an encrypted way.

For information on the confidentiality, please refer to Section 9.7.1.2, for information on the integrity, please refer to Section 9.7.1.3.

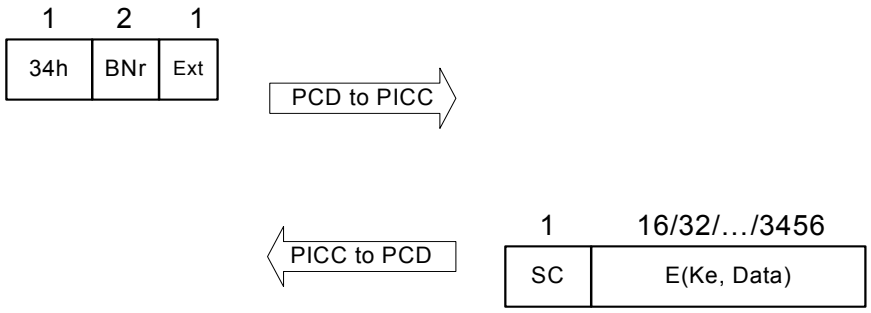


Fig 27. Read encrypted, no MAC on response, no MAC on command

Table 35. Command description Read encrypted, no MAC on response, no MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of the read encrypted, no MAC on response, MAC on command	34h
BNr	02h	Block Number of the first block to be read	see Table 111
Ext	01h	Number of blocks to be read	Sector Trailers do not count if Ext > 1.

Table 36. Response Read encrypted, no MAC on response, no MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
E(Ke, Data)	Multiple of 10h	The data to be read is encrypted with the session key as generated in the last authentication (see Section 9.7.2.1 or Section 9.7.2.3).	

9.7.3.6 Read encrypted, MAC on response, no MAC on command

This command offers the possibility to read the data from one or multiple blocks in an encrypted way. A MAC is used only on the response received.

For information on the confidentiality, please refer to Section 9.7.1.2, for information on the integrity, please refer to Section 9.7.1.3.

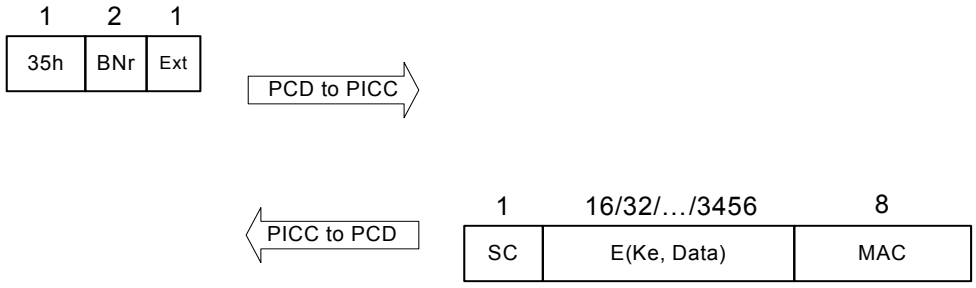


Fig 28. Read encrypted, MAC on response, no MAC on command

Table 37. Command description Read encrypted, MAC on response, no MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of the read encrypted, MAC on response, No MAC on command	35h
BNr	02h	Block Number of the first block to be read	see Table 111
Ext	01h	Number of blocks to be read	Sector Trailers do not count if Ext > 1.

Table 38. Response Read encrypted, MAC on response, no MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
E(Ke, Data)	Multiple of 10h	The data to be read is encrypted with the session key as generated in the last authentication (see Section 9.7.2.1 or Section 9.7.2.3).	
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

9.7.3.7 Read in plain, no MAC on response, no MAC on command

This command offers the possibility to read the data in plain from one or multiple blocks. A MAC is not used on the response and not on the command. For information on the confidentiality, please refer to Section 9.7.1.2, for information on the integrity, please refer to Section 9.7.1.3.

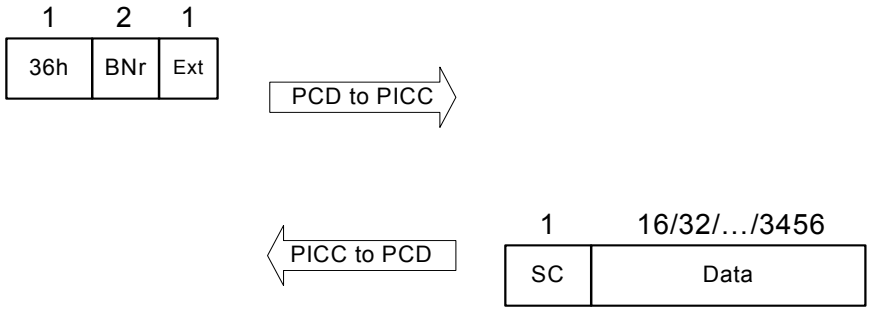


Fig 29. Read in plain, no MAC on response, no MAC on command

Table 39. Command description Read in plain, no MAC on response, no MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of the read in plain, MAC on response, MAC on command	36h
BNr	02h	Block Number of the first block to be read	see Table 111
Ext	01h	Number of blocks to be read	Sector Trailers do not count if Ext > 1.

Table 40. Response Read in plain, no MAC on response, no MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
Data	Multiple of 10h	The data to be read	

The read counter (R_Ctr) is incremented just prior to dispatch of the command.

9.7.3.8 Read in plain, MAC on response, no MAC on command

This command offers the possibility to read the data in plain from one or multiple blocks. A MAC is used on the response and not on the command. For information on the confidentiality, please refer to Section 9.7.1.2, for information on the integrity, please refer to Section 9.7.1.3.

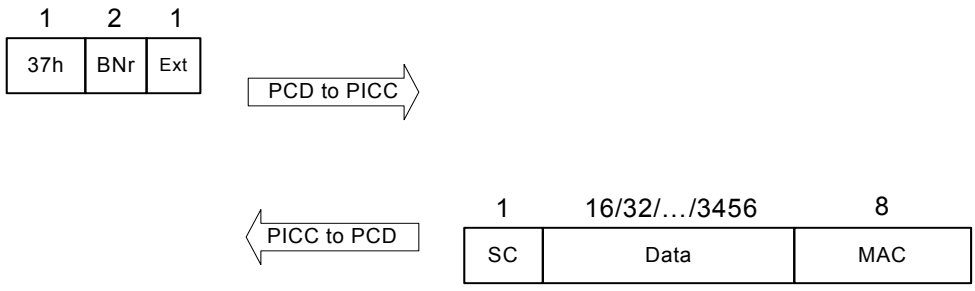


Fig 30. Read in plain, MAC on response, no MAC on command

Table 41. Command description Read in plain, MAC on response, no MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of the read in plain, MAC on response, no MAC on command	37h
BNr	02h	Block Number of the first block to be read	see Table 111
Ext	01h	Number of blocks to be read	Sector Trailers do not count in the numbers.

Table 42. Response Read in plain, MAC on response, no MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
Data	Multiple of 10h	The data to be read	
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

9.7.4 Write

The following options are available for the customer to choose from:

1. MAC on response, MAC on command data

- Data in plain
- Data encrypted

2. No MAC on response, MAC on command data

- Data in plain
- Data encrypted

The following table gives an overview of the available options resulting to the write command codes:

MAC on command	Plaintext	MAC on response	Command Code Write
Yes	No	No	A0h
Yes	No	Yes	A1h
Yes	Yes	No	A2h
Yes	Yes	Yes	A3h

9.7.4.1 Write encrypted, no MAC on response, MAC on command

This command offers the possibility to write the data to one or multiple blocks in an encrypted way. A MAC is only used on the command sent to the PICC. For information on the confidentiality, please refer to Section 9.7.1.2. For information on the integrity, please refer to Section 9.7.1.3.

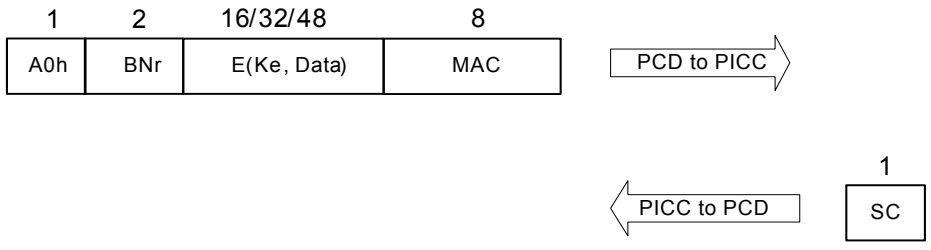


Fig 31. Write encrypted, no MAC on response, MAC on command

Table 43. Command description Write encrypted, no MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of Write encrypted, No MAC on response, MAC on command	A0h
BNr	02h	Block Number of the first to be written block	see Table 111
E(Ke, Data)	10h/20h/30h	Data encrypted with the current session key	
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

Table 44. Response Write encrypted, no MAC on response, MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112

9.7.4.2 Write encrypted, MAC on response, MAC on command

This command offers the possibility to write the data to one or multiple blocks in an encrypted way. A MAC is used on the command sent to the PICC and on the response received from the PICC. For information on the confidentiality, please refer to Section 9.7.1.2. For information on the integrity, please refer to Section 9.7.1.3.

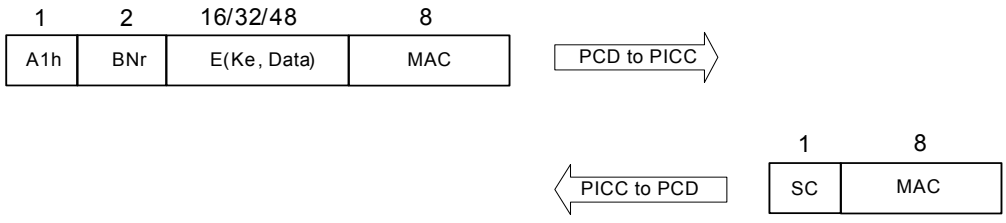


Fig 32. Write encrypted, MAC on response, MAC on command

Table 45. Command description Write encrypted, MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of Write encrypted, No MAC on response, MAC on command	A1h
BNr	02h	Block Number of the first to be written block	see Table 111
E(Ke, Data)	10h/20h/30h	Data encrypted with the current session key	
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

Table 46. Response Write encrypted, MAC on response, MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 111
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

9.7.4.3 Write in plain, no MAC on response, MAC on command

This command offers the possibility to write the data to one or multiple blocks in plain. A MAC is only used on the command sent to the PICC. For information on the confidentiality, please refer to Section 9.7.1.2. For information on the integrity, please refer to Section 9.7.1.3.

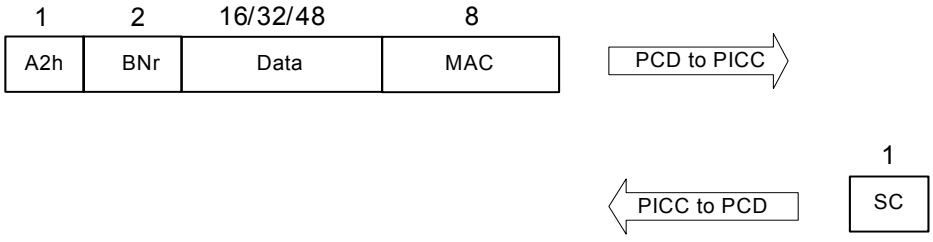


Fig 33. Write in plain, no MAC on response, MAC on command

Table 47. Command description Write in plain, no MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of Write encrypted, No MAC on response, MAC on command	A2h
BNr	02h	Block Number of the first to be written block	see Table 111
Data	10h/20h/30h	Data	
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

Table 48. Response Write encrypted, no MAC on response, MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112

9.7.4.4 Write in plain, MAC on response, MAC on command

This command offers the possibility to write the data to one or multiple blocks in plain. A MAC is used on the command sent to the PICC as well as on the response from the PICC. For information on the confidentiality, please refer to Section 9.7.1.2. For information on the integrity, please refer to Section 9.7.1.3.

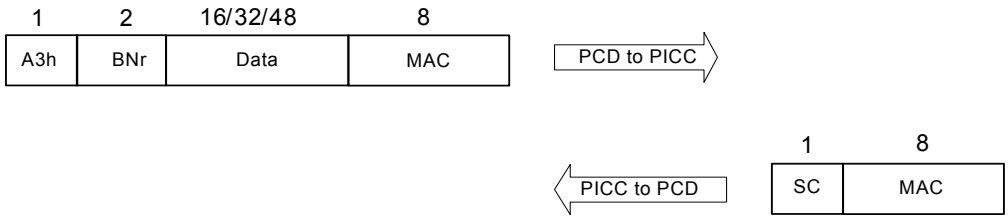


Fig 34. Write in plain, MAC on response, MAC on command

Table 49. Command description Write in plain, no MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of Write encrypted, No MAC on response, MAC on command	A3h
BNr	02h	Block Number of the first to be written block	see Table 111
Data	10h/20h/30h	Data	
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

Table 50. Response Write encrypted, no MAC on response, MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112

9.7.5 VALUE operations

Value operations offer the possibility to conveniently implement counters or purpose on top of backup management (see Section 9.1.2.1). The value (4 byte) is part of the value block (see Figure 5) and is one parameter in many commands used in the value operations. As the communication is encrypted and the value is less then 16 byte long, the value needs to be padded. The value is padded to a multiple of 128 bits in length by appending a single 80h and multipe 00h (see ISO/IEC 9797 section 2, padding method 2).

9.7.5.1 Increment encrypted, no MAC on response, MAC on command

This command offers the possibility to increment a value block (see Section 9.1.2.1) where the command is secured by a MAC calculated, but not on the response. For information on the confidentiality, please refer to Section 9.7.1.2. For information on the integrity, please refer to Section 9.7.1.3.

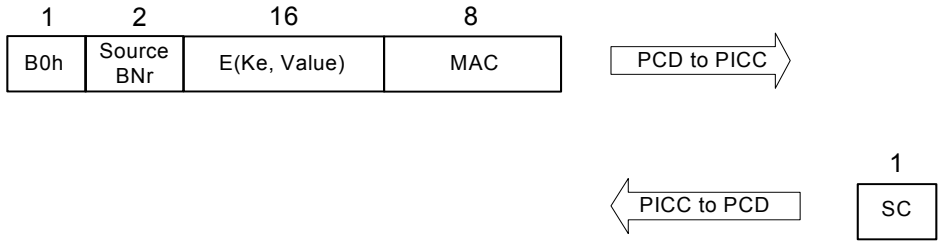


Fig 35. Increment encrypted, no MAC on response, MAC on command

Table 51. Command description Increment encrypted, no MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of Increment encrypted, no MAC on response, MAC on command	B0h
BNr	02h	Block Number of the block to be incremented	see Table 111
E(Ke, Value)	16	The value (4 byte), padded and encrypted with the session key from the current session.	The value block needs to be formatted as described in Section 9.1.2.1
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

Table 52. Response Increment encrypted, no MAC on response, MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112

9.7.5.2 Increment encrypted, MAC on response, MAC on command

This command offers the possibility to increment a value block (see Section 9.1.2.1) where the command is secured by a MAC calculated, but not on the response. For information on the confidentiality, please refer to Section 9.7.1.2. For information on the integrity, please refer to Section 9.7.1.3.

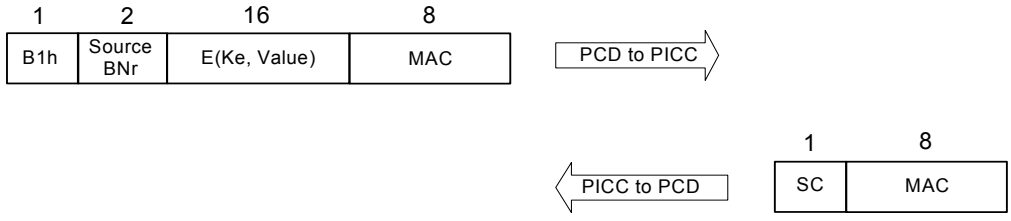


Fig 36. Increment encrypted, MAC on response, MAC on command

Table 53. Command description Increment encrypted, MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of Increment encrypted, MAC on response, MAC on command	B1h
BNr	02h	Block Number of the block to be incremented	see Table 111
		Number of block, whose content is to be used as a base for incrementing by the given value before storing the result in the Transfer Buffer.	
E(Ke, Value)	16	The value (4 byte), padded and encrypted with the session key from the current session.	The value block needs to be formatted as described in Section 9.1.2.1
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

Table 54. Response Increment encrypted, MAC on response, MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

9.7.5.3 Decrement encrypted, no MAC on response, MAC on command

This command offers the possibility to decrement a value block (see Section 9.1.2.1) where the command is secured by a MAC calculated, but not on the response. For information on the confidentiality, please refer to Section 9.7.1.2. For information on the integrity, please refer to Section 9.7.1.3.

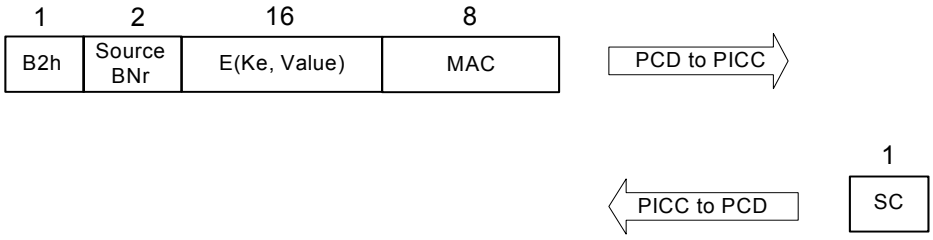


Fig 37. Decrement encrypted, no MAC on response, MAC on command

Table 55. Command description Decrement encrypted, no MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of Decrement encrypted, no MAC on response, MAC on command	B2h
BNr	02h	Block Number of the block to be decremented	see Table 111
		Number of block, which content is to be used as a base for decrementing by the given value before storing the result in the Transfer Buffer.	
E(Ke, Value)	10h	The value (4 byte), padded and encrypted with the session key from the current session.	The value block needs to be formatted as described in Section 9.1.2.1
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

Table 56. Response Decrement encrypted, no MAC on response, MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112

9.7.5.4 Decrement encrypted, MAC on response, MAC on command

This command offers the possibility to decrement a value block (see Section 9.1.2.1) where the command is secured by a MAC calculated, as well as on the response. For information on the confidentiality, please refer to Section 9.7.1.2. For information on the integrity, please refer to Section 9.7.1.3.

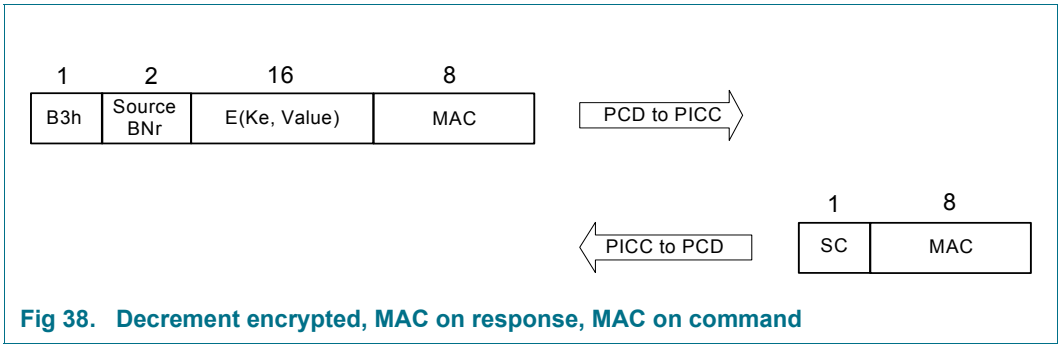


Fig 38. Decrement encrypted, MAC on response, MAC on command

Table 57. Command description Decrement encrypted, MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of Decrement encrypted, MAC on response, MAC on command	B3h
BNr	02h	Block Number of the block to be decremented	see Table 111
E(Ke, Value)	10h	The value block (4 byte), padded and encrypted with the session key from the current session.	The value block needs to be formatted as described in Section 9.1.2.1
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

Table 58. Response Decrement encrypted, MAC on response, MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

9.7.5.5 Transfer, no MAC on response, MAC on command

The Transfer command stores the content of the Transfer Buffer to the specified address. The Transfer command can only be performed to any block. The Transfer command can only be executed after an Increment, Decrement or Restore command. The command is secured by a MAC on a command. No MAC is calculated on the response. For information on the confidentiality, please refer to Section 9.7.1.2. For information on the integrity, please refer to Section 9.7.1.3.

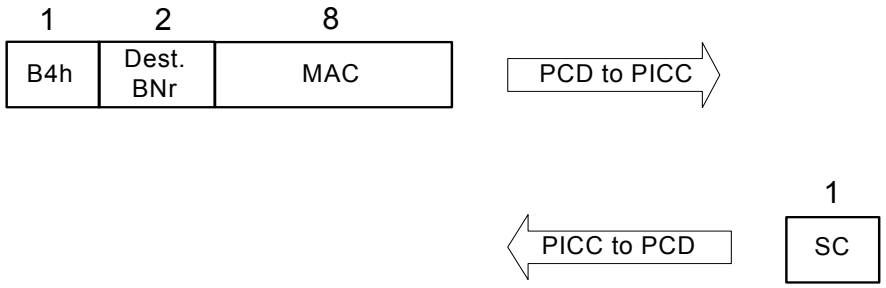


Fig 39. Transfer, no MAC on response, MAC on command

Table 59. Command description Transfer encrypted, no MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of Transfer encrypted, no MAC on response, MAC on command	B4h
Destination BNr	02h	Block Number of the block to be transferred	see Table 111
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

Table 60. Response Transfer encrypted, no MAC on response, MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112

9.7.5.6 Transfer, MAC on response, MAC on command

The Transfer command stores the content of the Transfer Buffer to the specified address. The Transfer command can be performed to any block. The Transfer command can only be executed after an Increment/Decrement or Restore command. The command is secured by a MAC on a command. A MAC is calculated on the response. For information on the confidentiality, please refer to Section 9.7.1.2. For information on the integrity, please refer to Section 9.7.1.3.

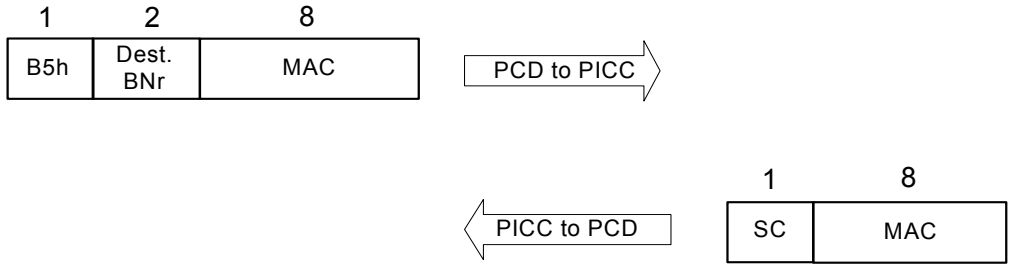


Fig 40. Transfer, MAC on response, MAC on command

Table 61. Command description Transfer encrypted, MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of Transfer encrypted, MAC on response, MAC on command	B5h
Destination BNr	02h	Block Number of the block to be transferred	see Table 111
		Number of block, whose content is to be replaced by the content of the Transfer Buffer.	
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

Table 62. Response Transfer encrypted, MAC on response, MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

9.7.5.7 Increment Transfer encrypted, no MAC on response, MAC on command

This command offers the possibility to make a combined increment and transfer within one command on a value block (see Section 9.1.2.1) where the command is secured by a MAC calculated, no MAC on the response. For information on the confidentiality, please refer to Section 9.7.1.2. For information on the integrity, please refer to Section 9.7.1.3.

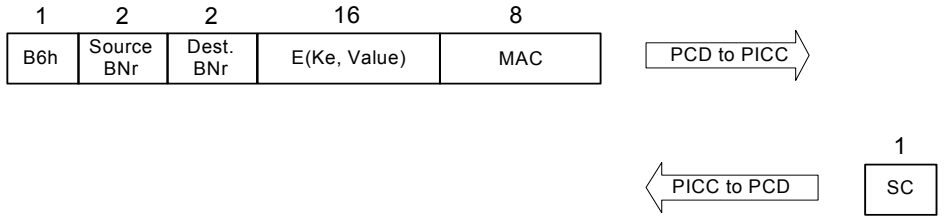


Fig 41. Increment Transfer encrypted, no MAC on response, MAC on command

Table 63. Command description Increment Transfer encrypted, no MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of Increment Transfer encrypted, no MAC on response, MAC on command	B6h
Source BNr	02h	Block Number of the source block.	see Table 111
Destination BNr	02h	Block Number of the to be written block	see Table 111
E(Ke, Value)	10h	The value (4 byte), padded and encrypted with the session key from the current session.	The value block needs to be formatted as described in Section 9.1.2.1
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

Table 64. Response Increment Transfer encrypted, no MAC on response, MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112

9.7.5.8 Increment Transfer encrypted, MAC on response, MAC on command

This command offers the possibility to make a combined increment and transfer within one command on a value block (see Section 9.1.2.1) where the command is secured by a MAC calculated, and as well as a MAC on the response. For information on the confidentiality, please refer to Section 9.7.1.2. For information on the integrity, please refer to Section 9.7.1.3.

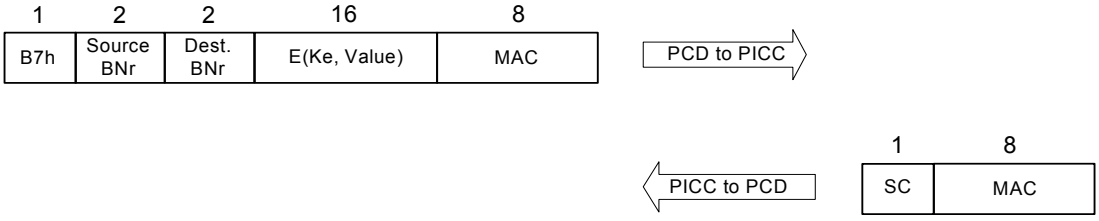


Fig 42. Increment Transfer encrypted, MAC on response, MAC on command

Table 65. Command description Increment Transfer encrypted, MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of Increment Transfer encrypted, MAC on response, MAC on command	B7h
Source BNr	02h	Block Number of the source block.	see Table 111
Destination BNr	02h	Block Number of the to be written block	see Table 111
E(Ke, Value)	10h	The value (4 byte), padded and encrypted with the session key from the current session.	The value block needs to be formatted as described in Section 9.1.2.1
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

Table 66. Response Increment Transfer encrypted, MAC on response, MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

9.7.5.9 Decrement Transfer encrypted, no MAC on response, MAC on command

This command offers the possibility to make a combined decrement and transfer within one command on a value block (see Section 9.1.2.1) where the command is secured by a MAC, but no MAC on the response. For information on the confidentiality, please refer to Section 9.7.1.2. For information on the integrity, please refer to Section 9.7.1.3.

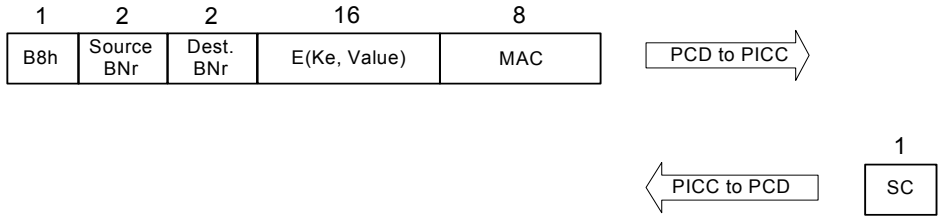


Fig 43. Decrement Transfer encrypted, no MAC on response, MAC on command

Table 67. Command description Decrement Transfer encrypted, no MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of Decrement Transfer encrypted, no MAC on response, MAC on command	B8h
Source BNr	02h	Block Number of the source block.	see Table 111
Destination BNr	02h	Block Number of the to be written block	see Table 111
E(Ke, Value)	10h	The value (4 byte), padded and encrypted with the session key from the current session.	The value block needs to be formatted as described in Section 9.1.2.1
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

Table 68. Response Decrement Transfer encrypted, no MAC on response, MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112

9.7.5.10 Decrement Transfer encrypted, MAC on response, MAC on command

This command offers the possibility to make a combined decrement and transfer within one command on a value block (see Section 9.1.2.1) where the command is secured by a MAC as well as one MAC on the response. For information on the confidentiality, please refer to Section 9.7.1.2. For information on the integrity, please refer to Section 9.7.1.3.

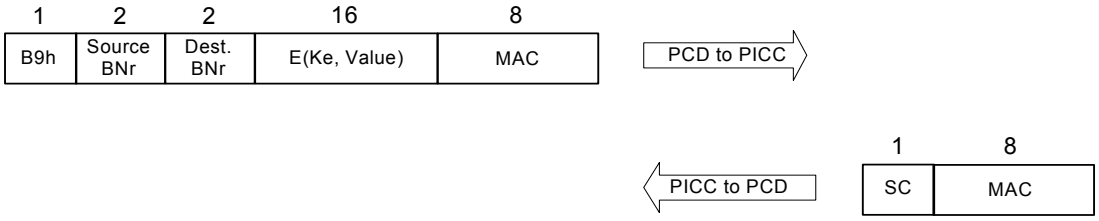


Fig 44. Decrement Transfer encrypted, MAC on response, MAC on command

Table 69. Command description Decrement Transfer encrypted, MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of Decrement Transfer encrypted, MAC on response, MAC on command	B9h
Source BNr	02h	Block Number of the source block.	see Table 111
Destination BNr	02h	Block Number of the block to be written to.	see Table 111
E(Ke, Value)	10h	The value (4 byte), padded and encrypted with the session key from the current session.	The value block needs to be formatted as described in Section 9.1.2.1
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

Table 70. Response Decrement Transfer encrypted, MAC on response, MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

9.7.5.11 Restore, MAC on response, MAC on command

The Restore command copies the Value found in the Value Block at the given address in the Transfer Buffer. The Restore command can only be performed to value blocks (see Section 9.1.2.1). The command is secured by a MAC on a command and a MAC is calculated on the response. For information on the confidentiality, please refer to Section 9.7.1.2. For information on the integrity, please refer to Section 9.7.1.3.

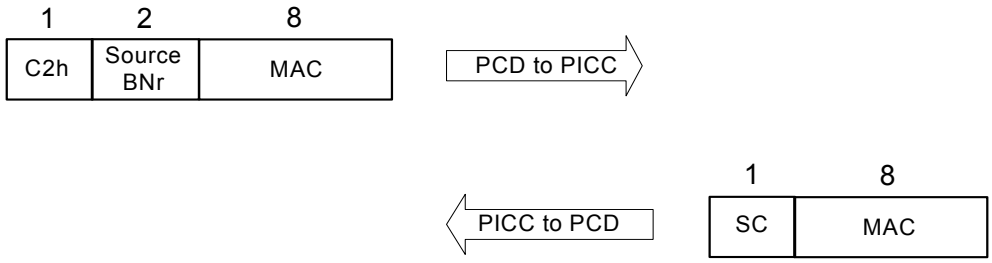


Fig 45. Restore, MAC on response, MAC on command

Table 71. Command description Restore encrypted, MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of Restore encrypted, MAC on response, MAC on command	C2h
Source BNr	02h	Block Number of the to be restored block	see Table 111
		Number of block, whose content is to be copied to the transfer buffer	
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

Table 72. Response Transfer encrypted, MAC on response, MAC on command

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

9.7.5.12 Restore encrypted, no MAC on response, MAC on command

The Restore command copies the Value found in the Value Block at the given address in the Transfer Buffer. The Restore command can only be performed to value blocks (see Section 9.1.2.1). The command is secured by a MAC on a command, no MAC is calculated on the response. For information on the confidentiality, please refer to Section 9.7.1.2. For information on the integrity, please refer to Section 9.7.1.3.

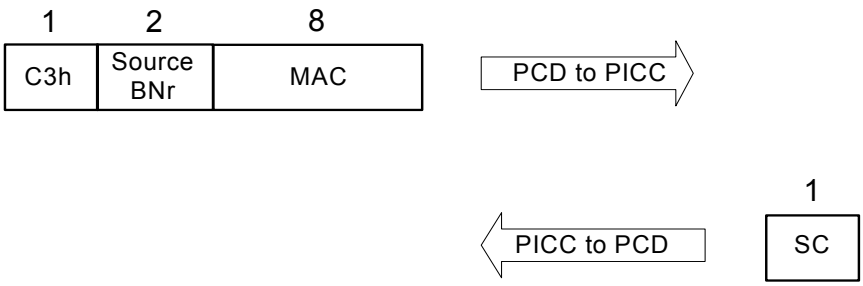


Fig 46. Restore Encrypted, no MAC on response, MAC on command

Table 73. Command description Restore encrypted, no MAC on response, MAC on command

Name	Length	Description	Value
Command Code	01h	Command Code of Restore encrypted, no MAC on response, MAC on command	C3h
Source BNr	02h	Block Number of the to be restored value block	see Table 111
		Number of block, which content is to be copied to the Transfer Buffer.	
MAC	08h	The MAC is calculated as described in as described in Section 9.7.1.3.	

Table 74. Response Restore encrypted, no MAC on response, MAC on command

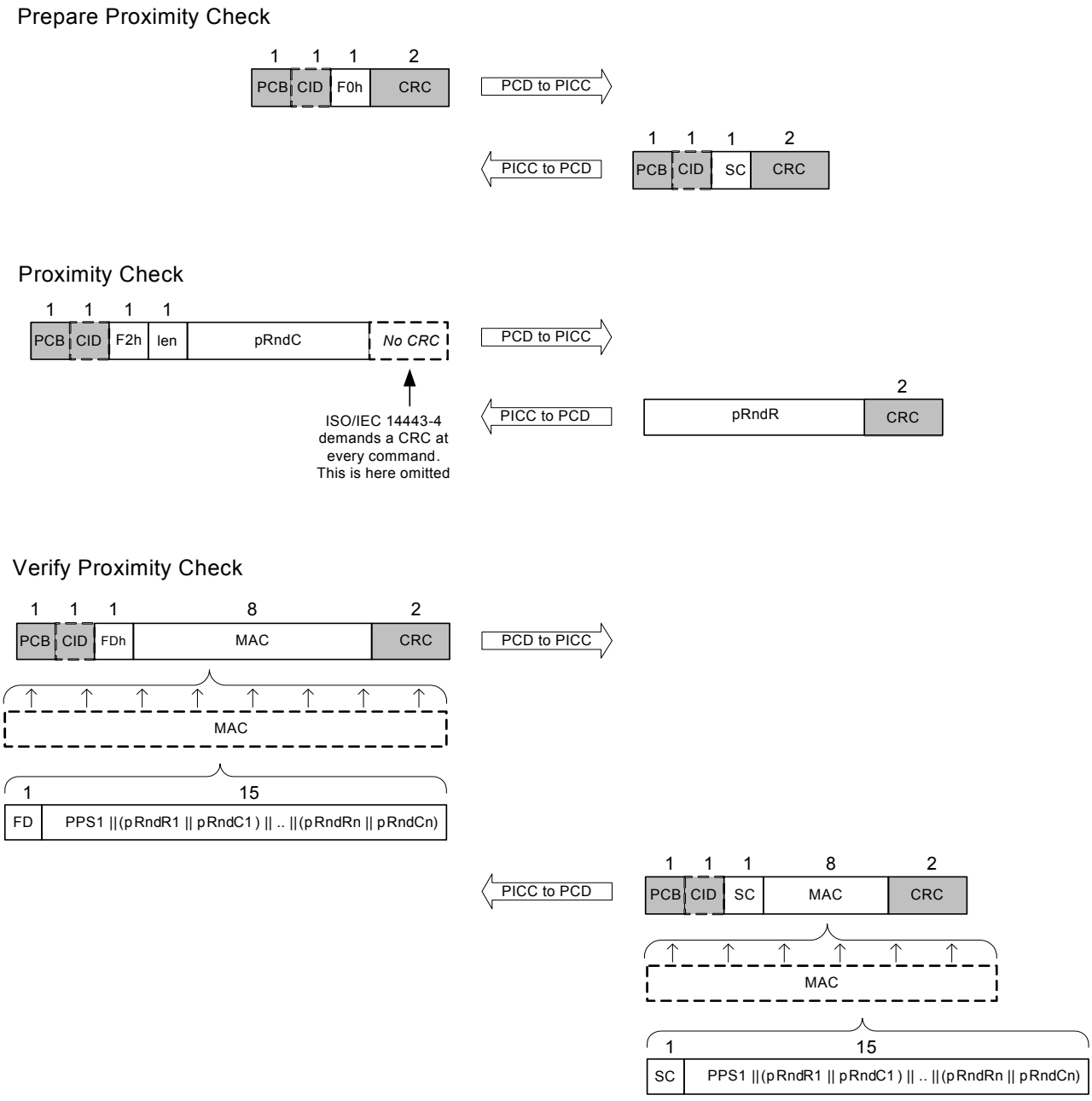
Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112

9.7.6 Proximity Check

Proximity checking is carried out by measuring the round trip time of a challenge-response interaction. If an attacker wants to mount a relay attack, then he will necessarily introduce delays. Depending on how large the delays are, they may be detected. The accuracy of the time measurement and the residual relay attack window that remains is dependent on the implementation of the reader.

Figure 47 gives an example of the messages exchanged during a Proximity Check.It shows the encapsulation of commands and responses with the ISO/IEC 14443-4 fields. It is done because one of the Proximity Check protocol command/response pairs drops some of the ISO/IEC 14443-4 fields. The Proximity Check consists of three commands:

- Prepare Proximity Check:
  The PICC is prepared to perform the Proximity Check.
- Proximity Check:
  The PICC answers with a prepared Random Number within a minimum time window. Between command sent and the response received exact measurements shall be taken by the PCD to detect attacks like replay attacks. The command may be repeated.
- Verify Proximity Check:
  The Random Numbers are verified using cryptographic methods.



In contradiction to all other figures of command sequences, here the protocol framing is visualized, as ISO/IEC 14443-4 is not totally followed.

Fig 47. Proximity Check

Table 75. Command description Prepare Proximity Check

Name	Length	Description	Value
Command Code	01h	Command Code of Prepare Proximity Check	F0h

Table 76. Response Prepare Proximity Check

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112

Table 77. Command description Proximity Check

Name	Length	Description	Value
Command Code	01h	Command Code Proximity Check	F2h
len	01h	Length of Random Number	01 to 07h
pRndC	01 to 07h	Random Number of the Reader	

Table 78. Response Proximity Check

Name	Length	Description	Value
pRndR	01 to 07h	Random Number of the PICC	
CRC	2	CRC calculated over all items in the command and the pRndR.	

Within the command Proximity Check, the ISO/IEC 14443-4 protocol is not followed. Therefore the CRCs and the CID in the response are omitted to measure in a more precise way. The proximity check command can be sent up to 7 times.

Table 79. Command description Verify Proximity Check

Name	Length	Description	Value
Command Code	01h	Command Code Verify Proximity Check	FDh
MAC	08h	The MAC is calculated over the following items in the following order, as described in Section 9.7.1 using the Proximity Check Key (see Table 111) or the current session key for MAC operation, K_{MAC}: 1. Command Code 2. PPS1 as defined in ISO/IEC 14443-4 3. Random Number of PICC	

Table 80. Response Verify Proximity Check

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
MAC	08h	The MAC is calculated over the following items in the following order, as described in Section 9.7.1using the Proximity Check Key (see Table 111) or the current session key for MAC operation, K_{MAC}: 1. Status Code 2. PPS1 as defined in ISO/IEC 14443-4 3. Random Number of the PCD	

The MAC within Verify Proximity Check can be calculated with one of two keys:

If the PICC is not authenticated (see Figure 17) the used key is the Proximity Check Key.

If the PICC is authenticated (see Figure 17) the used key is the current session key for MAC operation, the K_{MAC}.

9.7.7 Select Virtual Card Concept

MIFARE Plus is a product that is intended to be used for many years. As such a virtual card concept is introduced, which offers two major advantages:

- If Random ID shall be used, this concept offers the possibility to retrieve the UID in a very fast and secure from the PICC. This can be done by only sending one command, VC Support Last. This method is much faster than reading the Block 0 after an authentication, to retrieve the UID.

- One of the trends expected is that mobile phones and other personal devices will be used for making contactless transactions, in addition to the usage of traditional contactless cards (PICCs). This led to the concept of the Virtual Cards (VCs). A mobile phone could hold multiple VCs. MF1PLUSx0 includes only one Virtual Card.

The following commands are used within the Select Virtual Card Concept:

VC Support Command

The PCD sends such a command to the PICC for a Installation Identifier (IId, see Table 114) supported by the PCD infrastructure. This command is used to communicate which Installation Identifiers are supported by the PCD.

VC Support Last Command

The PCD communicates the Installation Identifier, as well as the PCD capabilities and a random challenge.The PICC returns the real UID of the card.This command is used to communicate if this particular installation identifier is supported by the PICC.

Select VC Command

The PCD confirms its intent to communicate with a given VC based on the response of the VC Support Last Command. The PICC returns with a status code.

Deselect VC Command

The virtual card is deselected.

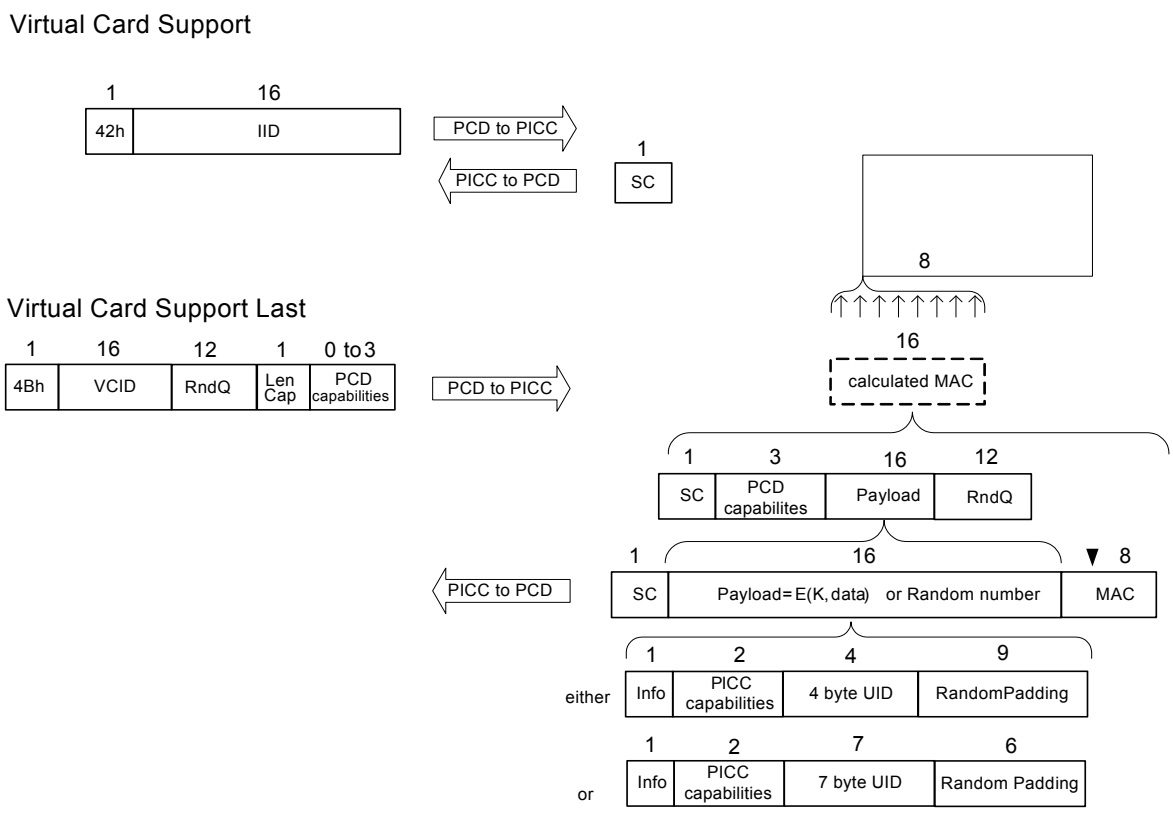


Fig 48. Virtual Card Support and Virtual Card Support Last

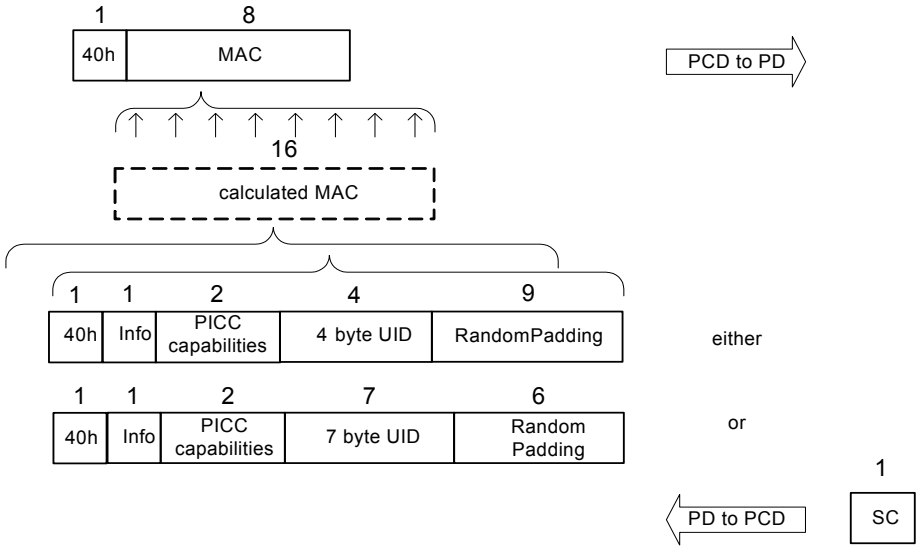


Fig 49. Select Virtual Card

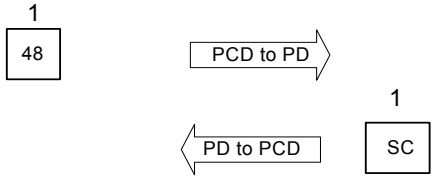


Fig 50. Deselect Virtual Card

Table 81. Command description Virtual Card Support

Name	Length	Description	Value
Command Code	01h	Command Code of Virtual Card Support	42h
IID	10h	Installation Identifier (see Table 111)	

Table 82. Response Virtual Card Support

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112

Table 83. Command description Virtual Card Support Last

Name	Length	Description	Value
Command Code	01h	Command Code of Virtual Card Support Last	4Bh
IID	10h	Installation Identifier (see Table 111)	
RndQ	0Ch	Random Number of the PCD	
LenCap	01h	Length of the Capabilities of the PCD	Between 0 and 3
Capabilities	00h-03h	Capabilities of the PCD	

Table 84. Response Virtual Card Support Last

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112
Payload = E(K, data)	10h	If the IID was not the same as stored in the PICC, it sends back a Random Number as a Payload. If the IID was equal, the following data has to be encrypted using the VC Polling Enc Key (see Table 111): 1. Info Byte (Default for 4 Byte UID: '83', default for 7 byte UID: '03') and PICC capabilities. The PICC1.1 is defined by NXP. The default value for 2K is '82' and for 4K: '83'. The PICC1.2 can be defined in the field configuration block , see Table 113. 2. Unique Identifier (UID) 3. Random Padding (9 byte for a 4Byte UID, 6 byte for a 7Byte UID)	
MAC	08h	The MAC is calculated using the VC Polling MAC Key (see Table 111) on the following items in the following order: Status Code 1. PCD Capabilities as sent by the PCD, the value can be defined upon the requirements of the PCD. 2. Payload as described above 3. Random Number of the PCD	

Table 85. Command description Select Virtual Card

Name	Length	Description	Value
Command Code	01h	Command Code Select Virtual Card	40h
MAC	08h	The MAC is calculated over the following items in the following order, as described in Section 9.7.1 using the Select VC card key (see Table 111): 1. Command Code 40h 2. Info and PICC capabilities as defined in Table 113 3. UID (4 byte or 7 byte depending on configuration) 4. Random Padding to a full 16 bytes string using same values as in the command (see Table 85)	

Table 86. Response Select Virtual Card

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112

Table 87. Command description Deselect Virtual Card

Name	Length	Description	Value
Command Code	01h	Command Code Deselect Virtual Card	48h

Table 88. Response Deselect Virtual Card

Name	Length	Description	Value
SC	01h	Status Code from the PICC	see Table 112

9.8 Exemplary transaction in security level 3

An exemplary transaction shall help in describing the functionality of MIFARE Plus in security level 3. The command examples do not include the IS0 14443-4 framing.The following commands are used in this order:

- First Authenticate (70h + 72h)
- Write encrypted MAC on command, MAC on response (A1h)
- Write encrypted MAC on command, MAC on response (A1h)
- Following Authenticate (76h + 72h)
- Read encrypted MAC on command, MAC on response (31h)
- Read encrypted MAC on command, MAC on response (31h)

9.8.1 First authenticate

This command is to authenticate with Key A for sector 2 (or block 4). The following parameters are set in the following way prior to the command:

- PCDcaps2: 2906 3410 0104h
- PICCcaps2: 0000 0000 0000h
- Maximum Session Read Counter: 0004h;
- Transaction Identifier: not exchanged yet
- Init Vector: 0000 0000 0000 0000 0000 0000 0000 0000h
- Key Number of Kx(Key A, sector 2): 4004h
- Value of Kx (Key A, sector 2): 8DDF F151 A6EF 6A7F E6D0 333A 42BE 21EEh
- W_Ctr: 0000h; R_Ctr: 0000h;

Table 89. Exemplary command First Authenticate

Value	Name	Description
70h	Command Code	Command Code First Authenticate, see Section 10.6
0440h	Key Number (LSB first!)	Key Number of the key to be authenticated with, see Section 10.7
06h	Length of PCD Capabilities	
2906 3410 0104h	PCDcaps2	See Section 10.10

Therefore the PCD sends the following stream to the PICC:

70044006290634100104

Table 90. Exemplary response First Authenticate

Value	Name	Description
90h	Status Code	Status Code, see Section 10.8
6DAF 3E03 08D6 6AB8 0AD9 BC7F 411A 34F2h	E(Kx, Rnd B)	The clear text of Rnd B is: B0E4 0C79 7C50 E1E4 8E88 BED0 4C9F 9579h

Therefore the PCD receives the following stream to the PICC:

906DAF3E0308D66AB80AD9BC7F411A34F2

Table 91. Exemplary command second step First Authenticate

Value	Name	Description
72h	Status Code	Command Code Second Step of Authentication, see Section 10.6
71F9 6656 2711 0CE1 D10D C2DF BE17 8E51 A2E7 2227 313F 0AFA 1BAB E84F BA57 D549h	E(Kx, Rnd A || Rnd B')	The clear text of Rnd A is: CFC1 0C4F 6305 3E15 0825 C8C7 E805 F302h The clear text of Rnd B' is: E40C 787C 50E1 E48E 88BE D04C 9F95 79B0h

Therefore the PCD sends the following stream to the PICC:

7271F9665627110CE1D10DC2DFBE178E51A2E72227313F0AFA1BABE84FBA57D549

Table 92. Exemplary response second step First Authenticate

Value	Name	Description
90h	Status Code	Status Code, see Section 10.8
673C AD29 070A FB6C 4C32 62AE EB4A 51BE 1FC7 D1B3 D108 23CF 1D4A 7E54 270B 1313	E(Kx, TI || Rnd A '||PICCcap2 || PCDCap2)	The clear text of Rnd A' is: C10C 4F63 053E 1508 25C8 C7E8 05F3 02CFh The clear text of the TI is: AABB CC24h PICCcaps2: 0000 0000 0000h PCDcaps2: 2906 3410 0104h

Therefore the PCD receives the following stream from the PICC:

90673CAD29070AFB6C4C3262AEEB4A51BEDE5219B04879F22BA96718DE63DBC87D

Out of the first authentication the First Authentication the following parameters are needed in the next commands:

- Transaction Identifier: AABB CC24h
- K_{ENC}: D13C DB09 CCD2 E42C E05E D7B8 B6EB C687h; see Section 9.7.2.1 for the calculation method.
- K_{MAC}: 72A8 2AEF 1A1E A4B8 695C 2608 22A2 A8E5h; see Section 9.7.2.1 for the calculation method.

The R_Ctr and W_Ctr as well as the session read counter are reset to 00h.

9.8.2 Write encrypted to block 9, MAC on message, MAC on response

This command is used to write data to block 9. The following parameters are used in the command:

- Transaction Identifier: AABB CC24h, as exchanged in Section 9.8.1.
- Init Vector encryption command: AABB CC24 0000 0000 0000 0000 0000 0000h
- K_{ENC}: D13C DB09 CCD2 E42C E05E D7B8 B6EB C687h, as generated in Section 9.8.1.
- K_{MAC}: 72A8 2AEF 1A1E A4B8 695C 2608 22A2 A8E5h, as generated in Section 9.8.1.
- Data to be written: 3214 A5F4 DE18 AEC8 DA6F 5033 32B7 10D7h
- W_Ctr: 0000h; R_Ctr: 0000h; (as it is the first command after Authentication)

Table 93. Exemplary command Write encrypted to block 9

Value	Name	Description
A1h	Command Code	Command Code Write encrypted, MAC on command, MAC on response, see Section 10.6
0900h	Block Number (LSB first)	Block Number of the block to be written, see Section 10.7
18A4 ABE3 07A2 03D8 7AA5 DBBB 0AF1 6F70h	E(Kx, Data)	Data: 3214 A5F4 DE18 AEC8 DA6F 5033 32B7 10D7h
BC43 05FE 729F BD03h	MAC	Payload, which goes into the MAC calculation: A1 0000 AABBCC24 0900 18A4ABE307A203D87AA5DBBB0AF16F70

Therefore the PCD sends the following stream to the PICC:

A1090018A4ABE307A203D87AA5DBBB0AF16F70BC4305FE729FBD03

Table 94. Exemplary response Write encrypted to block 9

Value	Name	Description
90h	Status Code	Status Code, see Section 10.8
746F E811 0EB2 1CA9h	MAC	Payload, which goes into the MAC calculation: 90 0100 AABBCC24h

Therefore the PCD receives the following stream from the PICC:

90746FE8110EB21CA9

9.8.3 Write encrypted to block 10, MAC on message, MAC on response

This command is used to write data to block 10. The following parameters are used in the command:

- Transaction Identifier: AABB CC24h, as exchanged in Section 9.8.1.
- Init Vector encryption command: AABBCC24 0000 0100 0000 0100 0000 0100h
- K_{ENC}: D13C DB09 CCD2 E42C E05E D7B8 B6EB C687h, as generated in Section 9.8.1.
- K_{MAC}: 72A8 2AEF 1A1E A4B8 695C 2608 22A2 A8E5h, as generated in Section 9.8.1.
- Data to be written: 02BB 2A18 BA7C 4B54 FC9F 8CAE 377F 5C1Ah
- W_Ctr: 0001h (as there was already on write command, see Section 9.8.2); R_Ctr: 0000h (as there was no read command since the first authentication)

Table 95. Exemplary command Write encrypted to block 9

Value	Name	Description
A1h	Command Code	Command Code Write encrypted, MAC on command, MAC on response, see Section 10.6
0A00h	Block Number (LSB first)	Block Number of the block to be written, see Section 10.7
103E 4B9E 7338 4F8F B79B 02F0 631B 4B45h	E(Kx, Data)	Data: 02BB 2A18 BA7C 4B54 FC9F 8CAE 377F 5C1Ah
E588 1768 83D3 908Fh	MAC	Payload, which goes into the MAC calculation:A1 0100 AABBCC24 0A00 103E 4B9E 7338 4F8F B79B 02F0 631B 4B45h

Therefore the PCD sends the following stream to the PICC:

A10A00103E4B9E73384F8FB79B02F0631B4B45E588176883D3908F

Table 96. Exemplary response Write encrypted to block 9

Value	Name	Description
90h	Status Code	Status Code, see Section 10.8
C2FB 0E11 9470 DF1Ch	MAC	Payload, which goes into the MAC calculation: 90 0200 AABBCC24h

Therefore the PCD receives the following stream from the PICC:

90C2FB0E119470DF1C

9.8.4 Following authenticate

This command is to authenticate with Key B for sector 4 (or block 11). The following parameters are set in the following way prior to the command:

- Maximum Session Read Counter: 0004h;
- Transaction Identifier: AABBCC24h
- Init Vector for encryption command: AABBCC24 0000 0200 0000 0200 0000 0200h
- Init Vector for encryption response: 0000 0200 0000 0200 0000 0200 AABBCC24h
- Key Number of Kx(Key A, sector 4): 4009h
- Value of Kx (Key B, sector 4): 1DD6 629D 8D44 3530 980E 4308 4A52 59FAh
- W_Ctr: 0002; R_Ctr: 0000h;

Table 97. Exemplary command Following Authenticate

Value	Name	Description
76h	Command Code	Command Code Following Authenticate, see Section 10.6
0940h	Key Number (LSB first)	Key Number of the key to be authenticated with, see Section 10.7

Therefore the PCD sends the following stream to the PICC:

760940

Table 98. Exemplary response Following Authenticate

Value	Name	Description
90h	Status Code	Status Code, see Section 10.8
1064 5305 C683 C4C3 3CA1 33F6 D067 ACFB	E(Kx, Rnd B)	The clear text of Rnd B is: F2DB 12E5 D255 D920 EA1A AEA6 A436 0799h Init vector used: 0000 0200 0000 0200 0000 0200 AABBCC24h

Therefore the PCD receives the following stream to the PICC:

9010645305C683C4C33CA133F6D067ACFB

Table 99. Exemplary command second step Following Authenticate

Value	Name	Description
72h	Status Code	Command Code Second Step of Authentication, see Section 10.6
D83C 0D0B AD1D F450 8220 1145 C40F 613A F1FF 30CF 0B0B 3829 29B6 7D11 B4F5 4481h	E(Kx, Rnd A || Rnd B')	The clear text of Rnd A is: 1E65 A479 94D0 A965 3308 61C2 4586 46CEh The clear text of Rnd B' is: DB12 E5D2 55D9 20EA 1AAE A6A4 3607 99F2h Init vector used: AABBCC24 0000 0200 0000 0200 0000 0200h

Therefore the PCD sends the following stream to the PICC:

72D83C0D0BAD1DF45082201145C40F613AF1FF30CF0B0B382929B67D11B4F54481

Table 100. Exemplary answer second step First Authenticate

Value	Name	Description
90h	Status Code	Status Code, see Section 10.8
88B9 1828 7009 94E7 E561 75EA 81D1 8CAFh	E(Kx, TI || PICCcap2 || Rnd A ')	The clear text of Rnd A' is: 65A4 7994 D0A9 6533 0861 C245 8646 CE1Eh Init vector used: 0000 0200 0000 0200 0000 0200 AABBCC24

Therefore the PCD receives the following stream from the PICC:

9088B91828700994E7E56175EA81D18CAF

Out of the following authentication, the keys need to be derived using the mechanism described in Section 9.7.2.1:

- K_{ENC}: 5941 6AD5 75A2 764E 8D0B 18FC C2E4 E24Fh; see Section 9.7.2.1 for the calculation method.
- K_{MAC}: BA90 F204 4172 6A3D DB57 7F7D 1EC9 C118h; see Section 9.7.2.1 for the calculation method.

The session read counter are reset to 00h, the W_Ctr, R_Ctr are maintained from the first authentication as well as the Transaction Identifier.

9.8.5 Read encrypted from block 17, MAC on message, MAC on response

This command is used to read data from block 17. The following parameters are used in the command:

- Transaction Identifier: AABB CC24h, as exchanged in Section 9.8.1.
- K_{ENC}: 5941 6AD5 75A2 764E 8D0B 18FC C2E4 E24Fh, as generated in Section 9.8.1.
- K_{MAC}: BA90 F204 4172 6A3D DB57 7F7D 1EC9 C118h, as generated in Section 9.8.1.
- W_Ctr: 0002h; R_Ctr: 0000h;

Table 101. Exemplary command Read encrypted from block 17

Value	Name	Description
31h	Command Code	Command Code Read encrypted, MAC on command, MAC on response, see Section 10.6
1100h	Block Number (LSB first)	Block Number (11h) of the block to be written, see Section 10.7
01h	Ext.	Number of blocks to be read (01)
5EB6 48C9 3B9E E9B8h	MAC	Payload, which goes into the MAC calculation: 31 0000 AABBCC24 110001h

Therefore the PCD sends the following stream to the PICC:

311100015EB648C93B9EE9B8

The init vector for encryption of the response is:

0100 0200 0100 0200 0100 0200 AABBCC24h

Table 102. Exemplary response Read encrypted from block 17

Value	Name	Description
90h	Status Code	Status Code, see Section 10.8
7597 11AF F8B6 E307 E71B 8A92 709C A6F0h	E(Kx, Data)	Data: 7856 3412 87A9 CBED 7856 3412 0AF5 0AF5h
BD72 CCD4 3B0C 7272h	MAC	Payload, which goes into the MAC calculation: 90 0100 AABBCC24 11 00 01 759711AFF8B6E307E71B8A92709CA6F0

Therefore the PCD receives the following stream from the PICC:

90759711AFF8B6E307E71B8A92709CA6F0FF1C4A5DDCE3168D

9.8.6 Read encrypted from block 18, MAC on message, MAC on response

This command is used to read data from block 18. The following parameters are used in the command:

- Transaction Identifier: AABB CC24h, as exchanged in Section 9.8.1.
- K_{ENC}: 5941 6AD5 75A2 764E 8D0B 18FC C2E4 E24Fh, as generated in Section 9.8.1.
- K_{MAC}: BA90 F204 4172 6A3D DB57 7F7D 1EC9 C118h, as generated in Section 9.8.1.
- W_Ctr: 0002h; R_Ctr: 0001h;

Table 103. Exemplary command Read encrypted from block 18

Value	Name	Description
31h	Command Code	Command Code Read encrypted, MAC on command, MAC on response, see Section 10.6
1200h	Block Number (LSB first)	Block Number of the block to be written, see Section 10.7
01h	Ext.	Number of blocks to be read (01)
AEA9 CA32 60C1 0734h	MAC	Payload, which goes into the MAC calculation: 31 0100 AABBCC24 1200 01h

Therefore the PCD sends the following stream to the PICC:

31120001AEA9CA3260C10734

The init vector for encryption of the response is: 0200 0200 0200 0200 0200 0200 AABBCC24h

Table 104. Exemplary response Read encrypted from block 18

Value	Name	Description
90h	Status Code	Status Code, see Section 10.8
8ADC C4C6 451A 23BB 6C1D EDE0 2DF3 AB72h	E(Kx, Data)	The cleartext: 6011 1600 9FEE E9FF 6011 1600 12ED 12EDh
0748 AF73 1448 9670h	MAC	Payload, which goes into the MAC calculation: 90 0200 AABBCC24 1200 01 8ADCC4C6451A23BB6C1DEDE02DF3AB72 h

Therefore the PCD receives the following stream from the PICC:

908ADCC4C6451A23BB6C1DEDE02DF3AB720748AF7314489670

10. Look-Up tables

10.1 Security level 0, 1, 2, 3: ISO/IEC 14443-3

Table 105. ISO/IEC 14443-3

Command	Description
REQA	REQA and ATQA are implemented fully according to ISO/IEC 14443-3.
WUPA	WAKE-UP is implemented fully according to ISO/IEC 14443-3.
ANTICOLLISION / SELECT Cascade level 1	The ANTICOLLISION and SELECT commands are implemented fully according to ISO/IEC 14443-3. The response is part 1 of the UID.
ANTICOLLISION / SELECT Cascade level 2 for 7 byte UID version	The ANTICOLLISION and SELECT commands are implemented fully according to ISO/IEC 14443-3. The response is part 2 of the UID.
HALT	HALT command is implemented fully according to ISO/IEC 14443-3

10.2 Security level 0,1,2, 3: ISO/IEC 14443-4

Table 106. ISO/IEC 14443-3

Command	Description
RATS	The response to the RATS command identifies the PICC type to the PCD.
PPS	The PPS command allows an individual selection of the communication baud rate between PCD and PICC. For MF1PLUSx0 it is possible to individually set the communication baud rate independently for both directions i.e. MF1PLUSx0 allows a non-symmetrical information interchange speed.
DESELECT	Deselection according to ISO/IEC 14443-4

Please find more information on ISO/IEC 14443 in Ref. 11 as well as on the settings of ATQA, SAK and ATS in Ref. 10.

10.3 Security level 0 command overview

Table 107. Security level 0 command overview

Command	HEX Code	Description
Write Perso	A8h	Pre Personalization of AES Keys and all blocks
Commit Perso	AAh	Switch to security level 1.

10.4 Security level 1 command overview

Table 108. Security level 1 command overview

MF1ICS50, MF1ICS70, MF1ICS20 commands	HEX Code	Description
MF Authenticate Key A	60h	Authentication with Key A
MF Authenticate Key B	61h	Authentication with Key B
MF Read	30h	Reading Data
MF Write	A0h	Writing Data
MF Increment	C1h	Incrementing a value
MF Decrement	C0h	Decrementing a value
MF Restore	C2h	Restoring a value
MF Transfer	B5h	Transferring a value

Table 108. Security level 1 command overview

MF1ICS50, MF1ICS70, MF1ICS20 commands	HEX Code	Description
Commands using backwards compatibility protocol, see Section 9.2.1		
MFP Following Authenticate	76h	Following Authentication, protocol used as described in Section 9.2.1
MFP Authenticate (part 2)	72h	2nd Step within the Authentication, protocol used as described in Section 9.2.1
Command Set for security level switch using ISO 14443-4 protocol		
First Authenticate (part 1)	70h	First Authentication
Authenticate (part 2)	72h	2nd Step within the Authentication
Authenticate	76h	Following Authentication

10.5 Security level 2 command overview

Table 109. Security level 2 command overview

Command	HEX Code	
Commands using backwards compatibility protocol, see Section 9.2.1		
MFP Following Authenticate	76h	Following Authentication, protocol used as described in Section 9.2.1
MFP Authenticate (part 2)	72h	2nd Step within the Authentication, protocol used as described in Section 9.2.1
MF1ICS50, MF1ICS70, MF1ICS20 commands		
MF Authenticate Key A	60h	Authentication with Key A
MF Authenticate Key B	61h	Authentication with Key B
MF Read	30h	Reading Data
MF Write	A0h	Writing Data
MF Decrement	C0h	Decrementing a value
MF Increment	C1h	Incrementing a value
MF Restore	C2h	Restoring a value
MF Transfer	B5h	Transferring a value
MFP Multi Block Read	38h	Reading multiple blocks (up to sector length)
MFP Multi Block Write	A8h	Writing multiple blocks (up to sector length)
Command Set for updating AES keys and configuration blocks as well as security level switch using ISO 14443-4		
First Authenticate (part 1)	70h	First Authentication
Authenticate (part 2)	72h	2nd Step within the Authentication
Authenticate	76h	Following Authentication
Write	A0h	Writing encrypted, No MAC on response, MAC on command,
Write MACed	A1h	Writing encrypted, MAC on response, MAC on command,

10.6 Security level 3 command overview

Table 110. Security level 3 command overview

Command	HEX code	Description
MIFARE Plus commands		
First Authenticate (part 1)	70h	First Authentication
Authenticate (part 2)	72h	2nd Step within the Authentication
Authenticate	76h	Following Authentication
ResetAuth	78h	Reset the authentication.
READ commands		
Read	30h	Reading encrypted, No MAC on response, MAC on command
Read MACed	31h	Reading encrypted, MAC on response, MAC on command
Read Plain	32h	Reading in plain, No MAC on response, MAC on command
Read Plain MACed	33h	Reading in plain, MAC on response, MAC on command
Read UnMACed	34h	Reading encrypted, No MAC on response, No MAC on command
Read UnMACed, Resp MACed	35h	Reading encrypted, No MAC on response, No MAC on command
Read Plain UnMACed	36h	Reading in plain, No MAC on response, No MAC on command
Read Plain UnMACed, Resp MACed	37h	Reading in plain, MAC on response, No MAC on command
WRITE commands		
Write	A0h	Writing encrypted, No MAC on response, MAC on command
Write MACed	A1h	Writing encrypted, MAC on response, MAC on command
Write Plain	A2h	Writing in plain, No MAC on response, MAC on command
Write Plain MACed	A3h	Writing in plain, MAC on response, MAC on command
VALUE operations		
Increment	B0h	Incrementing a value encrypted, No MAC on response, MAC on command
Increment MACed	B1h	Incrementing a value encrypted, MAC on response, MAC on command
Decrement	B2h	Decrementing a value encrypted, No MAC on response, MAC on command
Decrement MACed	B3h	Decrementing a value encrypted, MAC on response, MAC on command
Transfer	B4h	Transferring a value, No MAC on response, MAC on command
Transfer MACed	B5h	Transferring a value, MAC on response, MAC on command

Table 110. Security level 3 command overview *…continued*

Command	HEX code	Description
Increment Transfer	B6h	Combined incrementing and transferring a value encrypted, No MAC on response, MAC on command
Increment Transfer MACed	B7h	Combined incrementing and transferring a value encrypted, MAC on response, MAC on command
Decrement Transfer	B8h	Combined decrementing and transferring a value encrypted, No MAC on response, MAC on command
Decrement Transfer MACed	B9h	Combined decrementing and transferring a value encrypted, MAC on response, MAC on command
Restore	C2h	Restoring a value, No MAC on response, MAC on command
Restore MACed	C3h	Restoring a value, MAC on response, MAC on command
Proximity Check and VC Concept		
Prepare Proximity Check	F0h	Prepare for the Proximity Check
Proximity Check	F2h	Perform the precise measurement for the proximity check
Verify Proximity Check	FDh	Verify the proximity check
Virtual Card Support	42h	Check, if the Virtual Card Concept is supported
Virtual Card Support Last	4Bh	Select the Virtual Card and retrieve the UID
Select Virtual Card	40h	Select the Virtual Card
Deselect Virtual Card	48h	Select the Virtual Card

10.7 Key and block number overview

The key and block numbers are always transmitted according to Little Endian: the LSB first. Therefore the address (e.g. the ATS Information) is transmitted as '02 B0'.Keys and blocks can only be updated after authentication with the previous key are the dedicated key, the write command needs to be secured by encryption.

Table 111. Key and block number overview

Command	HEX address	Description
Blocks and data		
MIFARE Data/Value Blocks MIFARE Sector Trailers	00 00h to 00 7Fh	Sector 0 to 31
MIFARE Data/Value Blocks MIFARE Sector Trailers	00 80h to 00 FFh	Sector 32 to 39
MFP Configuration Block	B0 00h	Defines the number of unmaced commands as well as if plain communication is possible (see Section 10.10)
Installation Identifier	B0 01h	Installation Identifier as used in VC concept (see Section 9.7.7). The installation Identifier can be requested from NXP.
ATS Information	B0 02h	The 'Answer to Select' Information
Field Configuration Block	B0 03h	Defines if Proximity Check is mandatory and if RandomID shall be enabled (see Section 10.9)
Keys		
AES Sector Keys	40 00h to 40 3Fh	AES Sector Keys for sector 0 to 31. The second byte defines the sector number and which key (Key A or Key B) is used. Key A =sector number multiplied by 2 Key B = sector number multiplied by 2 + 1 E.g. Key A for sector 2 has the number: 40 04
AES Sector Keys	40 40h to 40 4Fh	AES Sector Keys for sector 32 to 39. The second byte defines the sector number and which key (Key A or Key B) is used. Key A =sector number multiplied by 2 Key B = sector number multiplied by 2 + 1
Originality Key	80 00h	The originality is personalised by NXP to the IC and cannot be changed. As the value of the key is not distributed outside of NXP, the authentication with this key is only possible with a special prepared SAM, supplied by NXP.
Card Master Key	90 00h	Can be used to change the Level Switch Keys as well as the MFP Configuration Key.
Card Configuration Key	90 01h	Can be used to change the Field Configuration Block
Level 2 Switch Key	90 02h	Key to switch from level 1 to level 2
Level 3 Switch Key	90 03h	Key to switch from level 2 to level 3
SL1 Card Authentication Key	90 04h	Key to do one additional AES authentication in security level 1
Select VC Key	A0 00h	Key to perform Select VC

Table 111. Key and block number overview *…continued*

Command	HEX address	Description
Proximity Check Key	A0 01h	Key to verify the Proximity Check
VC Polling ENC Key	A0 80h	Select VC Polling ENCKey
VC Polling MAC Key	A0 81h	Select VC Polling MAC Key

10.8 Error code overview

Table 112. Error code overview

Error code	HEX address	Description
(Not) Acknowledge (NACK/ACK) (see Section 9.2.1)		
Transfer cannot be granted	0h	Transfer cannot be granted within the current authentication.
Wrong CRC Value in 1st exchanged package	5h	
Wrong CRC Value in 2nd exchanged package	1h	
Conditions of use not satisfied	4h	One of the following reasons can lead to this error code: Block Number out of Range Access condition violation Write block 0 is not possible Transfer Buffer is empty
Acknowledge	Ah	Command is successful
Error Codes (see Section 9.2.2)		
Authentication Error	06h	Access Conditions not fulfilled The block is to be accessed does not exist The block is to be accessed is not a value block and an operation is performed that only work on value blocks
Command Overflow	07h	Too many read or write commands in the session or in the transaction
Invalid MAC	08h	Invalid MAC in command or response
Invalid Block Number	09h	Block Number is not valid
Not Existing Block Number	0Ah	Invalid Block number, not existing Block Number
Conditions of use not satisfied	0Bh	The current command is not allowed on the requested block, or any of the requested blocks, when authorization is done with the key that was used in the latest authentication step.
Length Error	0Ch	Length Error
General Manipulation Error	0Fh	Failure in the operation of the PICC, e.g. cannot write to the data block Increment command or Increment Transfer command causes overflow Decrement command or Decrement Transfer command causes underflow
Success Code	90h	ok

10.9 Field configuration block

The field configuration block configures the available command set to the customer. The field configuration block can be changed after authentication with the Configuration Key (see Table 49). The block consisting of 16 bytes are not all used. Bytes as marks as 'RFU' are not checked and used by the PICC. The Field configuration block can be changed using an encrypted write command after authentication with the Card Configuration Key (see Table 49).The items are in stored in the block in the same order as in the following table.

Table 113. Field configuration block

Item	Length	Description
RFU	01h	RFU, set to 00h
UseRID	01h	Indicates if Random ID is used. Valid values are: 55h indicating Random ID not used AAh indicating Random ID is used
PCM	01h	Indicates if Proximity Check Command needs to be used before any sector is addressed. Valid values are: 55h indicating Proximity Check is not used AAh indicating Proximity Check is used
RFU	01h	RFU, set to 00h
PICCCap1.2	01h	PICC capabilities used during Virtual Card Selection, default value is 00h.
RFU	04h	RFU, set to 00h
PICCCap2.5	01h	PICC capabilities used during First Authentication, default value is 00h.
PICCCap2.6	01h	PICC capabilities used during First Authentication, default value is 00h.
RFU	05h	RFU, set to 00h

10.10 MFP configuration block

The MFP configuration block is used to define if plain communication can be used (see Default Access Byte 4) and if a MAC is needed on a read command sent to the PICC. The MFP configuration block can be changed using an encrypted write command after authentication with the Master Key (see Table 49). The block consisting of 16 bytes are not all used. Bytes as marks as 'RFU' are not checked and used by the PICC.The items are in stored in the block in the same order as in the following table

Table 114. MFP configuration block

Item	Length	Description
Maximum Unmaced Commands	01h	It defines if and how many unmaced read commands can be used. There are three values: 1. 00h MAC on Read Mandatory, this is the default value. 2. FFh MAC on Read optional and number of Read only limited to Read Counter R_Ctr 3. nnh Number of read commands, which can be conducted within one transaction, where MAC on command sent is optional.
Access Byte for plain read	01h	Default Access Byte 4, defines on which block plain communication can be used, see Section 10.11. Default value is 0Fh.
RFU	0Eh	RFU, set to 00h

10.11 Access byte for plain communication

The Default Access Condition 0 is a access condition byte, which is only available in security level 3 and defines if Plain Read and Plain Write can be used for a block. The access byte is set on byte 4 in the sector trailer of each sector (see Section 9.1.3).

Table 115. Access byte for plain read for 4 block sector

Bit No.	Block No.	Description
7	Invert (Block 3)	If set to 0, reading in plain is possible for Block 3 of the sector.
6	Invert (Block 2)	If set to 0, reading in plain is possible for Block 2 of the sector.
5	Invert (Block 1)	If set to 0, reading in plain is possible for Block 1 of the sector.
4	Invert (Block 0)	If set to 0, reading in plain is possible for Block 0 of the sector.
3	Block 3	If set to 1, reading in plain is possible for Block 3 of the sector.
2	Block 2	If set to 1, reading in plain is possible for Block 2 of the sector.
1	Block 1	If set to 1, reading in plain is possible for Block 1 of the sector.
0	Block 0	If set to 1, reading in plain is possible for Block 0 of the sector.

Table 116. Access byte for plain read for 16 block sector

Bit No.	Block No.	Description
7	Invert (Block 15)	If set to 0, reading in plain is possible for Block 3 of the sector.
6	Invert (Block 10 to 14)	If set to 0, reading in plain is possible for Block 2 of the sector.
5	Invert (Block 5 to 9)	If set to 0, reading in plain is possible for Block 1 of the sector.
4	Invert (Block 0 to 4)	If set to 0, reading in plain is possible for Block 0 of the sector.
3	Block 15	If set to 1, reading in plain is possible for Block 3 of the sector.
2	Block 10 to 14	If set to 1, reading in plain is possible for Block 2 of the sector.
1	Block 5 to 9	If set to 1, reading in plain is possible for Block 1 of the sector.
0	Block 0 to 4	If set to 1, reading in plain is possible for Block 0 of the sector.

So if all blocks within one sector shall be readable in plain, the value is 0Fh.

11. Limiting values

Table 117. Limiting values [1][2]

In accordance with the Absolute Maximum Rating System (IEC 60134).

Symbol	Parameter	Conditions		Min	Max	Unit
I_I	input current			-	30	mA
P_{tot}/pack	total power dissipation per package			-	200	mW
T_{stg}	storage temperature range			−55	125	°C
T_{amb}	anbient temperature			−25	70	°C
V_{ESD}	electrostatic discharge voltage		[3]	2	-	kV
I_{lu}	latch-up current			±100	-	mA

[1] Stresses above one or more of the limiting values may cause permanent damage to the device

[2] Exposure to limiting values for extended periods may affect device reliability

[3] MIL Standard 883-C method 3015; Human body model: C = 100 pF, R = 1.5 kΩ

12. Characteristics

Table 118. Characteristics [1][2]

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
C_i	input capacitance	T_{amb} = 22 °C, f_i = 13.56 MHz; 2.8 V RMS	[3]	14.96	17.0	19.04	pF
f_i	input frequency			-	13.56	-	MHz
EEPROM characteristics							
t_{ret}	retention time	T_{amb} = 22 °C		10	-	-	year
$N_{endu(W)}$	write endurance	T_{amb} = 22 °C, excluding anti tearing for AES keys or sector trailers in security level 3		100000	200000	-	cycle

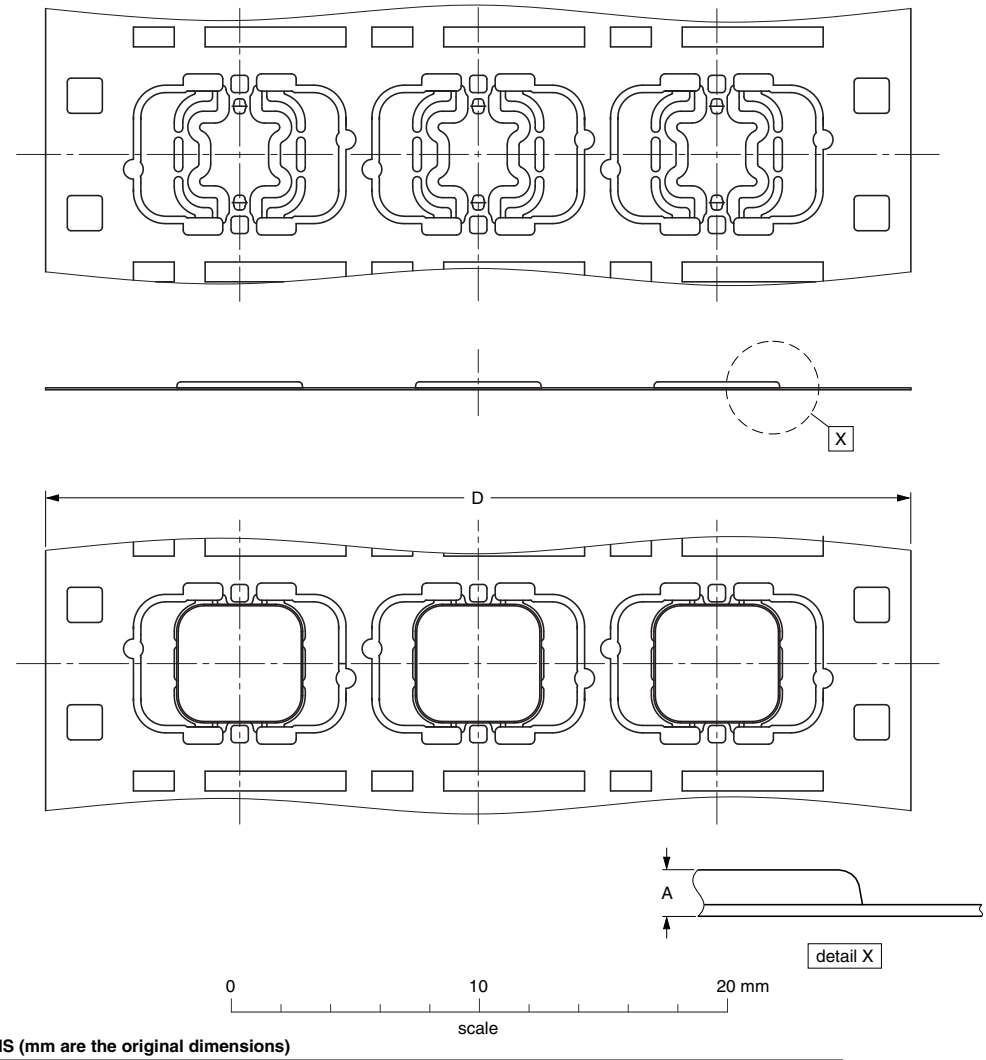
[1] Stresses above one or more of the values may cause permanent damage to the device

[2] Exposure to limiting values for extended periods may affect device reliability

[3] LCR meter

13. Package outline

PLLMC: plastic leadless module carrier package; 35 mm wide tape **SOT500-2**



DIMENSIONS (mm are the original dimensions)

UNIT	A(1) max.	D	
mm	0.33	35.05 34.95	For unspecified dimensions see PLLMC-drawing given in the subpackage code.

Note

1. Total package thickness, exclusive punching burr.

OUTLINE VERSION	REFERENCES				EUROPEAN PROJECTION	ISSUE DATE
	IEC	JEDEC	JEITA			
SOT500-2	- - -	- - -	- - -			~~03-09-17~~ 06-05-22

Fig 51. Package outline SOT500-2

14. Abbreviations

Table 119. Abbreviations and symbols

Acronym	Description
AES	Advanced Encryption Standard
ACK	Acknowledge
EEPROM	Electrically Erasable Programmable Read-Only Memory
E(Key A, Data)	The data is encrypted using Key A.
FWT	Frame Waiting Time
IID	Installation Identifier
LSB	Least Significant Byte
MAC	Message Authentication Code
MSB	Most Significant Byte
NV	Non Volatile Memory
NACK	Not Acknowledge
PCD	Proximity Coupling Device (’Contactless Reader’)
PICC	Proximity Integrated Circuit Card(’Contactless Card’ or ’PICC’)
PPS	Protocol Parameter Selection
RATS	Request Answer To Select
REQA	Request Answer
RID	UID0 = 08h, Random number in UID 1... UID 3
SAK	Select Acknowledge, Type A
SAM	Secure Access Module
SC	Status Code
UID	Unique Identifier, Type A
VC	Virtual Card, one MIFARE Plus PICC is one virtual card
WUPA	Wake Up Protocol A
||	concatenated
[bXX..bYY]	The xx bit of the stream to the yy bit of the stream. 00 is the least significant bit.

15. References

[1] **Data sheet —** MF1ICS50 Functional Specification, BL-ID Doc. No. 001054

[2] **Data sheet —** MF1ICS20 Functional Specification, BL-ID Doc. No. 132212

[3] **Data sheet —** MF1ICS70 Functional Specification, BL-ID Doc. No. 043542

[4] **Data sheet —** MF3ICD81 MIFARE DESFire Functional Specification, BL-ID Doc. No. 134034

[5] **Data sheet —** MF0ICU1 Functional Specification, BL-ID Doc. No. 028635

[6] **Data sheet —** MF0ICU2 Functional Specification, BL-ID Doc. No. 137610

[7] **User manual —** MF3ICD81 Guidance, Delivery and Operation Manual, BL-ID Doc No. 146934

[8] **Application note —** MIFARE DESFire - Implementation hints and examples, BL-ID Doc. No. 094531

[9] **Application note —** MF0ICU1 Application Note MIFARE Ultralight features and hints, BL-ID Doc. No. 073121

[10] **Application note —** MIFARE Type Identification Procedure, BL-ID Doc. No. 18430

[11] **Application note —** ISO 14443 PICC Selection, BL-ID Doc. No. 130820

[12] **NIST Special Publication 800-38A —** 2001 Edition NIST Special Publication 800-38B

[13] **NIST Special Publication 800-38B —** Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication

[14] **ISO/IEC Standard —** ISO/IEC 14443 Identification cards - Contactless integrated circuit cards - Proximity cards

16. Revision history

Table 120. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
163714	20090325	Objective data sheet	-	163713
Modifications:	Version 1.4 • New name for the product: MIFARE Plus X • Update of init vector handling in Section 9.7.1.2. • Update of PICCCaps used in Section 9.8.			
163713	20090223	Objective data sheet	-	163712
Modifications:	Version 1.3.1 • Security Level 3 Example (see Section 9.8) • Including Wafer Spec Addendum and Module Specification (see Section 7.1, Section 7.2, Section 7.3, Section 7.4, Section 7.5, Section 7.6) • Including Originality Function (see Section 9.1.7) Version 1.3.2 • New State Diagrams (see Figure 11, Figure 12, Figure 17) and descriptions.			
163712	20081212	Objective data sheet	-	163711
Modifications:	• General update			
163711	20081201	Objective data sheet	-	163710
Modifications:	• General update • MAC truncation is changed (see Section 9.7.1.3) • Authentication included in Security Level 1 (see Section 9.5) • Key Numbering (see Section 10.7)			
163710	20081031	Objective data sheet	-	MF1ICS6001

17. Legal information

17.1 Data sheet status

Document status[1][2]	Product status[3]	Definition
Objective [short] data sheet	Development	This document contains data from the objective specification for product development.
Preliminary [short] data sheet	Qualification	This document contains data from the preliminary specification.
Product [short] data sheet	Production	This document contains the product specification.

[1] Please consult the most recently issued document before initiating or completing a design.

[2] The term 'short data sheet' is explained in section "Definitions".

[3] The product status of device(s) described in this document may have changed since this document was published and may differ in case of multiple devices. The latest product status information is available on the Internet at URL http://www.nxp.com.

17.2 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

Short data sheet — A short data sheet is an extract from a full data sheet with the same product type number(s) and title. A short data sheet is intended for quick reference only and should not be relied upon to contain detailed and full information. For detailed and full information see the relevant full data sheet, which is available on request via the local NXP Semiconductors sales office. In case of any inconsistency or conflict with the short data sheet, the full data sheet shall prevail.

17.3 Disclaimers

General — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in medical, military, aircraft, space or life support equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors accepts no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

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

Terms and conditions of sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, including those pertaining to warranty, intellectual property rights infringement and limitation of liability, unless explicitly otherwise agreed to in writing by NXP Semiconductors. In case of any inconsistency or conflict between information in this document and such terms and conditions, the latter will prevail.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

Quick reference data — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

17.4 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

MIFARE — is a trademark of NXP B.V.

MIFARE Plus — is a trademark of NXP B.V.

18. Contact information

For more information, please visit: **http://www.nxp.com**

For sales office addresses, please send an email to: **salesaddresses@nxp.com**

19. Tables

20. Figures

21. Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 25 March 2009
Document identifier: 163714

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 25 March 2009
Document identifier: 163714