MF0AES(H)20

MIFARE Ultralight AES contactless limited-use IC

Rev. 3.2 — 28 March 2023 Product data sheet

1 General description

MIFARE Ultralight AES is a smart IC serving the requirements of limited use applications for contactless tickets and RFID key cards managed by one single entity. MIFARE Ultralight AES is offering a powerful mix between performance, security, privacy and flexibility. It addresses the needs of limited use applications such as public transport, hospitality, access, event ticketing and loyalty applications, by expanding the MIFARE Ultralight ticketing IC portfolio and adds Advanced Encryption Standards (AES) into it.

MIFARE Ultralight AES comes with AES-128 cryptography and enables product protection mechanisms in terms of product authenticity and integrity. Its enhanced feature and command set enables efficient implementations and offers flexibility in system designs and is a perfect contactless ticketing expansion to the smart card contactless IC families such as MIFARE DESFire or MIFARE Plus. Based on these parameters the MIFARE Ultralight AES is a trusted platform targeting the secure authentication of people with an intuitive convenient user experience.

MIFARE Ultralight AES is fully compliant with the contactless proximity smart card protocol according to ISO/IEC 14443-3 making it compatible with the majority of existing contactless infrastructure devices. Its contactless performance supports advanced user convenience and reading distances up to 10 cm (depending on various parameters as e.g. field strength and antenna geometry).

MIFARE Ultralight AES has a 4 byte per one page memory structure with a total user memory of 144-byte. To protect sensitive data against unauthorized access, MIFARE Ultralight AES offers a 3-pass mutual authentication based on AES with a 128-bit key. For data integrity protection an optional CMAC calculation for commands and response can be enabled, following NIST Special Publication 800-38B, see [15]. Besides the data protection MIFARE Ultralight AES serves the option to protect one out of the three independent 24-bit one-way counters by an AES authentication. To prevent undefined counters values due to tear-off in the field or originating from interrupted programming cycles an advanced anti-tearing support is implemented.

MIFARE Ultralight AES is also ready to support contactless applications addressing privacy sensitive use-cases. With its optional support of Random ID, it enables compliance with latest user data protection regulations.

MIFARE Ultralight AES enables check of the manufacturing origin of a ticket by verification of an asymmetric signature retrieved from the IC using the UID and an ECC-based originality signature. The default NXP signature can be overwritten with a customer-specific signature during personalization. The purpose of originality check is to identify mass penetration of none-genuine MIFARE Ultralight AES ICs into an infrastructure.

MIFARE Ultralight AES is designed to support smart ticket antenna designs with a 17 pF input capacitance as well as smaller form factors for key fobs, tags or wristbands by providing 50 pF input capacitance. This is offered by FFC deliveries and MOA8 modules to ensure high user convenience throughout different form factors.

1.1 Contactless energy and data transfer

Communication to MIFARE Ultralight AES is established by connection of the IC to an antenna. The MIFARE Ultralight AES supports either 17 pF or 50 pF resonance capacitor. The contactless interface is compliant to ISO/IEC 14443A-2/ -3, see [1] , [2] with low power consumption enabling operating distances of up to 10 cm. Together with the fast start-up time it allows reliable and robust detection at terminals. As soon as the MIFARE Ultralight AES credential with applied antenna is positioned in the RF field, the RF communication interface allows the transmission of the data with a baud rate of 106 kbit/s.

1.2 Anti-collision

An anti-collision function allows to operate more than one card in the field simultaneously. The anti-collision algorithm selects each card individually and ensures that the execution of a transaction with a selected card is performed correctly without interference from another card in the field.

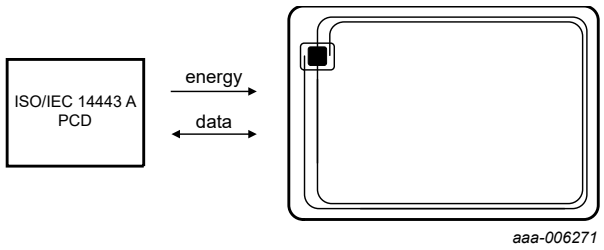


Figure 1. Contactless System

The anti-collision function is based on an IC individual serial number called Unique IDentifier. The MIFARE Ultralight AES supports double size UID according to ISO/IEC 14443-3, see [2].

1.3 Simple integration and user convenience

MIFARE Ultralight AES offers specific features designed to improve integration and user convenience:

- The data access protection with AES authentication based on a key length of 128-bit
- Optional CMAC protection for message integrity
- The fast read capability allows reading the complete user memory with only one FAST_READ command, therefore reducing the overhead in high throughput production environments
- The improved RF performance allows for more flexibility in the choice of shape, dimension and materials
- The Random ID support for enhanced user privacy compliant with latest user data protection regulations

The MIFARE Ultralight AES is designed for simple integration and advanced user convenience with superior ticketing transactions times.

1.4 NFC Forum Tag 2 Type compliance

MIFARE Ultralight AES can be configured to comply to the NFC Forum Tag 2 Type technical specification, see [20] and allows to enable NDEF data structure configurations as specified in [21].

1.5 Security and privacy

- Common Criteria certification: EAL3+ (AVA_VAN.2)
- 3-pass mutual AES authentication based on a key length of 128-bit
- Configurable secure messaging communication mode
  - CMAC for message integrity protection according to NIST Special Publication 800-38B, see [15].
- Three independent 24-bit one-way counters with optional AES authentication protection of one counter
- Unique 7-byte IDentifier for each device
- Random ID (optional) for enhanced privacy. Compliant to ISO14443-3
- 32-bit user programmable OTP area
- Field programmable read-only locking function per page for the first 512 bit
- Read-only locking per block of 2 pages for the memory above 512 bit
- Pre-programmed ECC-based originality signature, offering the possibility for customizing and permanently locking
- AES-based originality key leveraging the AES authentication to check the NXP origin of the IC via NXP tools

Note: MF0AES(H)20 comes with an external CC EAL3+ certification targeting basic attack potential (AVA_VAN.2). Hence, the contactless IC does not claim to be completely resistant. In case of broader protection is required, products with a higher security certification should be considered.

1.6 Naming conventions

Table 1. Naming conventions

MF0AES(H)xyffdpp	Description
MF0	MIFARE Ultralight family
AES	AES … Advanced Encryption Standard
(H)	One-character identifier for input capacitance ... 17 pF H ... 50 pF
x	One-character identifier for user memory size 2 … 144 byte
y	0 … EV0
f	One-character identifier for UID type 0 … 7B UID
f	One-character identifier for the source 1 ... Single source 0 ... Multi source
Dpp	Fixed plus two-character identifier for the package type UF ... bare die, 75 µm thickness UD ... bare die, 120 µm thickness A8 ... MOA8 contactless module

2 Features and benefits

- Contactless transmission of data and supply energy compliant to ISO/IEC 14443 -2/ -3 A, see [1]and [2]
- Operating frequency of 13.56 MHz
- Data transfer of 106 kbit/s
- Data integrity of 16-bit CRC, parity, bit coding, bit counting
- Anti-collision function allows to operate more than one card in the field simultaneously
- Low power consumption enabling operating distances of up to 10 cm (depending on various parameters as e.g. field strength and antenna geometry)
- Fast start-up time for reliable and robust detection
- Support of double size (7-byte) Unique IDentifiers (UID) and optionally Random ID (RID) according to ISO/IEC 14443-3 A, [2]
- Optional CMAC calculation for data integrity protection
- 3-pass mutual authentication with AES based on a 128-bit key
- ECC-based originality signature, offering the possibility for customizing and permanently locking
- Fast read command
- 17 pF and 50 pF input capacitance to support high user convenience throughout different form factors
- Fast counter transaction

2.1 Memory

- 144 bytes freely available Read/Write user memory, organized in 36 pages with 4 bytes per page
- 4 bytes One Time Programmable (OTP) access bits
- Anti-tearing support for counters, Lock bits, OTP bits
- Field programmable read-only locking function per page for the first 16 pages
- Field programmable read-only locking function above the first 16 pages per 2 pages
- Configurable AES authentication for data access protection with optional limit of unsuccessful attempts
- Configurable data protection access rights for available user memory
- Pre-programmed ECC-based originality signature, offering the possibility for customizing and permanently locking
- Compatibility to allow NFC Type 2 Tag compliant configurations
- Data retention time of 10 years
- Write endurance of 100.000 cycles

3 Applications

The target applications of the MIFARE Ultralight AES are primarily designed for single or limited use applications such as:

- Public transport for limited use ticketing
- Hospitality RFID basic guest card
- Event ticketing
- Electronic voucher
- Loyalty tickets

4 Quick reference data

Table 2. Characteristics of MIFARE Ultralight AES

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
f_i	input frequency		-	13.56	-	MHz
C_i	input capacitance for MF0 AESxy [1]	IC and MOA8	-	17	-	pF
	input capacitance for MF0 AESHxy [1]	IC and MOA8	-	50	-	pF
EEPROM characteristics						
t_{ret}	retention time	T_{amb} = 22 °C	10	-	-	year
$N_{endu(W)}$	write endurance	T_{amb} = 22 °C	100	-	-	kcycle

[1] T_{amb} = 22 °C, f = 13.56 MHz, V_{LaLb} = 2 V RMS

5 Ordering information

Table 3. Ordering information MF0AES(H)xy

Type number	Package	Description	Memory	Input cap	UID
MF0AES2001DUD	FFC	8 inch wafer (laser diced, 120 µm) [1]	144 byte	17 pF	7 byte
MF0AES2001DUF	FFC	8 inch wafer (laser diced, 75 µm) [1]	144 byte	17 pF	7 byte
MF0AES2000DA8	MOA8	Plastic leadless module carrier package [2]	144 byte	17 pF	7 byte
MF0AESH2001DUD	FFC	8 inch wafer (laser diced, 120 µm) [1]	144 byte	50 pF	7 byte
MF0AESH2001DUF	FFC	8 inch wafer (laser diced, 75 µm) [1]	144 byte	50 pF	7 byte
MF0AESH2000DA8	MOA8	Plastic leadless module carrier package [2]	144 byte	50 pF	7 byte

[1] On FFC (Film Frame Carrier) with electronic fail die marking according to SECSII format
[2] Plastic leadless module carrier package; 35 mm wide tape

6 Block diagram

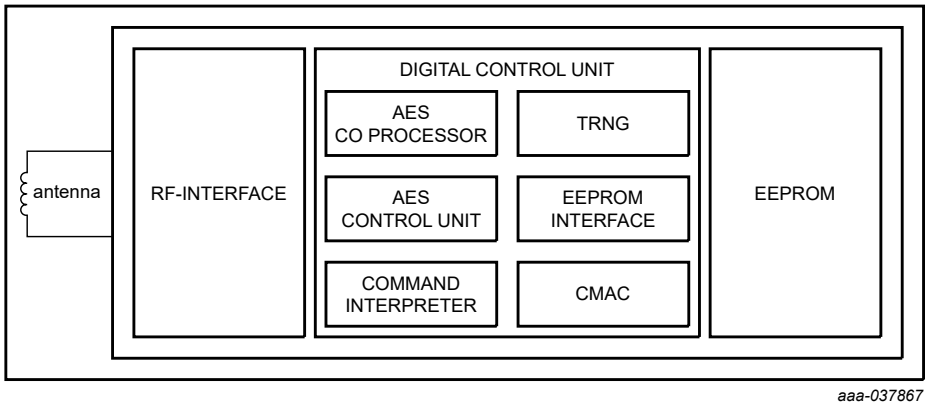


Figure 2. Block diagram

7 Pinning information

7.1 Wafer delivery

The pinning of the dies on the Film Frame Carrier (FFC) is shown in section "Bare die outline", see Table 4.

Table 4. Pin allocation table

Pin	Symbol	Description
LA	LA	Antenna coil connection LA
LB	LB	Antenna coil connection LB
GND	GND	Ground Pin (disconnected)
TEST	TEST	Test Pin (disconnected)

7.2 Smart card contactless module

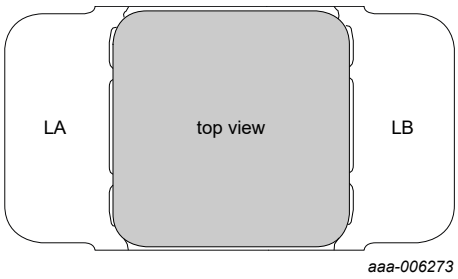


Figure 3. Contact assignments for SOT500-4 (MOA8)

Table 5. Pin allocation table

Antenna contacts	Symbol	Description
LA	LA	Antenna coil connection LA
LB	LB	Antenna coil connection LB

8 Functional description

8.1 Block description

The MIFARE Ultralight AES IC consists of a 240 byte EEPROM, RF-Interface and the Digital Control Unit. Energy and data are contactless transferred between the contactless reader resp. Proximity Coupled Device (PCD) and Proximity Integrated Circuit Card (PICC). PICC antenna which consists of a coil with a few turns directly connects to the MIFARE Ultralight AES contactless IC.

No further external components are necessary. For details on antenna design please refer to the document, see [7].

- RF-Interface:
  - Modulator/Demodulator
  - Rectifier
  - Clock Regenerator
  - Power On Reset
  - Voltage Regulator
- Anti-collision support: multiple cards may be selected and managed in sequence
- True Random Number Generator (TRNG)
- Crypto coprocessor: Advanced Encryption Standard (AES)
- Crypto control unit: controls Crypto coprocessor operations
- Command Interpreter: processes memory access commands that the MIFARE Ultralight AES supports
- EEPROM-Interface
- MIFARE Ultralight AES EEPROM: 240 byte, organized in 60 pages of 4 bytes per page.
  - First 16 byte are for manufacturer data, Lock byte 0 and 1, One-Time-Programmable (OTP) page
  - 144 byte are user programmable read/write memory
  - 80 byte configuration pages and RFU

8.2 RF interface

The RF interface is based on the ISO/IEC 14443 Type A standard, see [1] and [2].

During operation, the contactless reader (PCD) generates an RF field. This RF field must always be present with short pauses for data communication. It is used for both communication and as power supply for the tag.

For both directions of data communication, there is one start bit at the beginning of each frame. Each byte is transmitted with an odd parity bit at the end, except for REQA and WUPA command. The LSB of the byte with the lowest address of the selected block is transmitted first. The maximum length of a PCD to PICC frame for AUTH_Part 2 is 280 bits excluding parity bits. The maximum length for a fixed size PICC to PCD frame is 208 bits for READ command with CMAC without parity bits. The FAST_READ response has a variable frame length depending on the start and end address parameters. When issuing this command, take the maximum frame length of the PCD into account.

For a multi-byte parameter, the least significant byte is always transmitted first. As an example, take reading from the memory using the READ command, byte 0 from the addressed block is transmitted first. It is then followed by bytes 1 to byte 3 out of this block. The same sequence continues for the next block and all subsequent blocks.

8.3 Data integrity

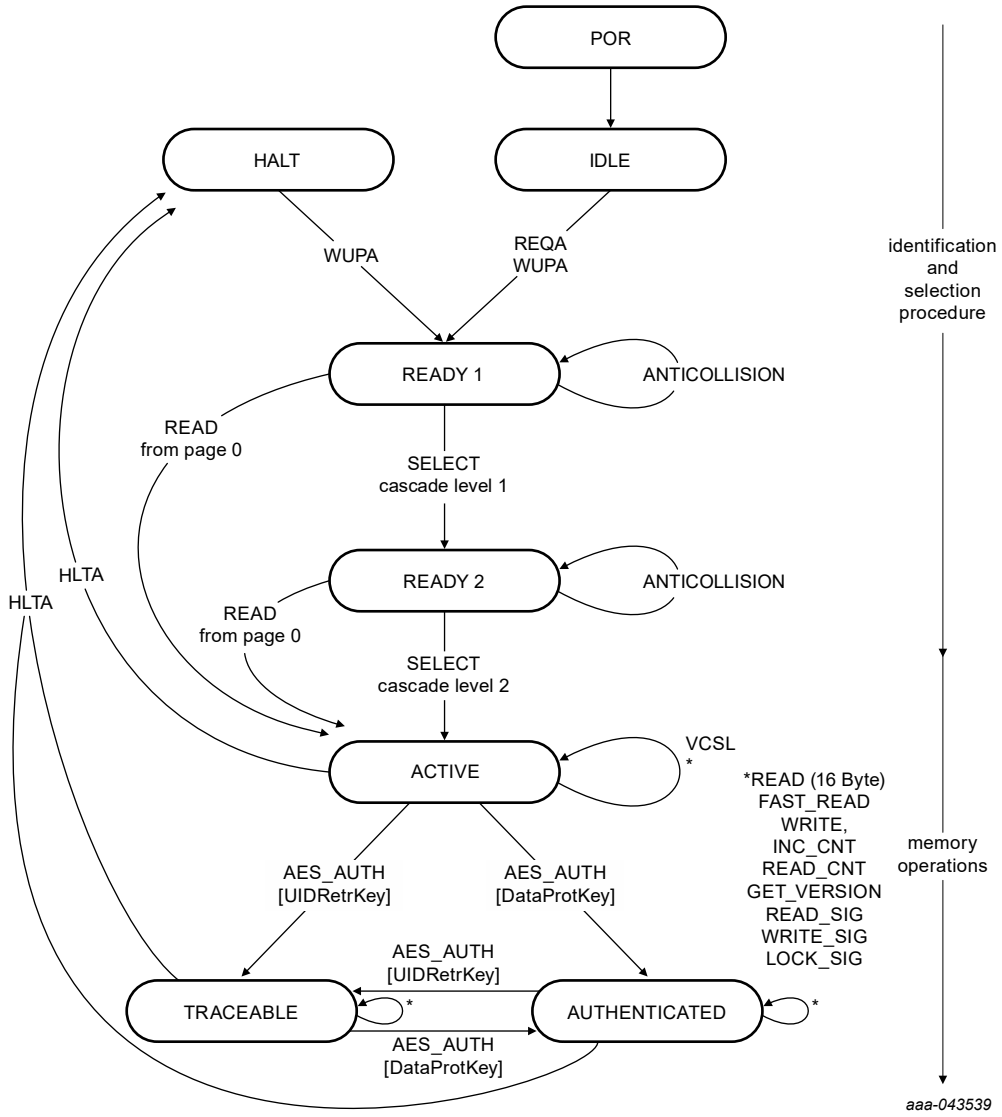
Following mechanisms are implemented in the contactless communication link between contactless reader and smart ticket contactless IC to ensure very reliable data transmission:

- User commands and responses
- 16-bit Cyclic Redundancy Check (CRC) according to ISO/IEC 14443-3, see [2], calculated over all preceding bytes in the same communication frame
- Parity bit for each byte
- Bit count checking and bit coding to distinguish between "1", "0", and no information
- Channel monitoring (protocol sequence and bit stream analysis)
- Configurable secure messaging communication mode to apply CMAC for message integrity protection

8.4 Communication principle

The contactless reader initiates the commands and the Command Interpreter of the MIFARE Ultralight AES processes them. The command response is depending on the state of the IC and for memory operations also on the access conditions valid for the corresponding page.

For a correct implementation of an anti-collision procedure, see [2].



Remark: In all states, the command interpreter returns to the idle state on receipt of an unexpected command. If the IC was previously in the HALT state, it returns in that state.

Remark: The VCSL command is only allowed in the ACTIVE state.

Remark: In ACTIVE state, all operations are allowed which are not requiring authentication.

Remark: In TRACEABLE state, once standard 7 byte UID is activated, there is not difference to ACTIVE state except that VCSL command is not supported in TRACEABLE state. Once RID is activated, then on top of all operations allowed in ACTIVE state in TRACEABLE state also all privacy sensitive operations reading UID bytes and originality signature are allowed.

Remark: In AUTHENTICATED state, all operations are allowed like in ACTIVE or TRACEABLE state except VCSL command. On top in AUTHENTICATED state, the access to protected memory element is allowed and access to counter #2 is allowed if configured as authentication protected.

Figure 4. State diagram

8.4.1 IDLE and HALT

After Power-On-Reset (POR), MIFARE Ultralight AES switches to IDLE state. It only exits this state when a REQA or a WUPA command is received from the contactless reader. Any other data received while in this state is interpreted as an error and MIFARE Ultralight AES remains in the IDLE state. After a correctly executed HLTA

command i.e. out of the ACTIVE, TRACEABLE or AUTHENTICATED state, the default waiting state changes from the IDLE state to the HALT state. This state can then be exited with a WUPA command only.

Please refer to [2] for implementation hints for a card polling algorithm that respects relevant timing specifications from ISO/IEC 14443 Type A.

8.4.2 READY1

In this state, the contactless reader resolves the first part of the UID (3 bytes) or complete Random ID using the ANTICOLLISION or SELECT commands in cascade level 1. This state is exited correctly after execution of either of the following commands:

- SELECT command from cascade level 1: once double side UID is configured the PCD switches the MIFARE Ultralight AES into READY2 state where the second part of the UID is resolved. The response of the MIFARE Ultralight AES to the cascade level 1 SELECT command is the SAK byte with value 04h. It indicates that the UID has not been completely received by the contactless reader and another anti-collision level is required. Once Random ID is configured the PCD switches the MIFARE Ultralight AES into ACTIVE state. In this case SAK answer will indicate completion of the anti-collision process.
- READ command (from address 0): all anti-collision mechanisms are bypassed and the MIFARE Ultralight AES switches directly to the ACTIVE state.

Remark: If more than one MIFARE Ultralight AES is in the field of the contactless reader, a read from address 0 will cause a collision because of the different serial numbers, but all MIFARE Ultralight AES devices will be selected. Any other data received in state READY1 state is interpreted as an error and the MIFARE Ultralight AES falls back to its waiting state (IDLE or HALT, depending on its previous state).

8.4.3 READY2

In this state, the MIFARE Ultralight AES supports the contactless reader in resolving the second part of its UID (4 bytes) with the cascade level 2 ANTICOLLISION command. This state is usually exited using the cascade level 2 SELECT command.

Alternatively, READY2 state can be skipped using a READ command (from block address 00h) as described in state READY1.

The response of the MIFARE Ultralight AES to the cascade level 2 SELECT command is the select acknowledge (SAK) byte. In accordance with ISO/IEC 14443, this byte indicates if the anti-collision cascade procedure has finished. The MIFARE Ultralight AES is now uniquely selected and only this device communicates with the contactless reader even when other contactless devices are present in the reader field. If more than one MIFARE Ultralight AES is in the reader field, a READ command from address 0 selects all MIFARE Ultralight AES devices. In this case, a collision occurs.

Any other data received when the device is in this state is interpreted as an error and, depending on its previous state, the MIFARE Ultralight AES returns to either the IDLE state or HALT state.

8.4.4 ACTIVE

Allowed memory operations are operated in the ACTIVE state. Operations with a required authentication will be rejected.

The ACTIVE state is exited with either HLTA or AUTHENTICATE command. Upon reception of HLTA command, MIFARE Ultralight AES transits to the HALT state. Similarly MIFARE Ultralight AES transits to the AUTHENTICATED/TRACEABLE state after successful 3-pass mutual authentication using the AUTHENTICATE command with [DataProtKey] or [UIDRetrKey] respectively.

Any other unsupported data received when the device is in ACTIVE state is interpreted as an error. Depending on its previous state, the MIFARE Ultralight AES returns to either the IDLE state or HALT state.

8.4.5 TRACEABLE

In TRACEABLE state following operations are allowed depending on activated UID type:

Once standard 7 byte UID is activated, there is not difference to ACTIVE state except that VCSL command is not supported in TRACEABLE state.

Once RID is activated, then on top of all operations allowed in ACTIVE state in TRACEABLE state also all privacy sensitive operations reading UID bytes and originality signature are allowed.

Secure messaging is supported in TRACEABLE state.

The TRACEABLE state is exited with either HLTA or AUTHENTICATE command. Upon reception of HLTA command, MIFARE Ultralight AES transits to the HALT state. Similarly MIFARE Ultralight AES transits to the AUTHENTICATED/ACTIVE state after successful 3-pass mutual authentication using the AUTHENTICATE command with [DataProtKey] or [OriginalityKey] respectively.

Any other unsupported data received when the device is in this state is interpreted as an error. Depending on its previous state returns to either the IDLE state or HALT state.

8.4.6 AUTHENTICATED

In the AUTHENTICATED state, all operations on memory pages, which are configured as authentication protected, can be accessed. Also all operations that are allowed in TRACEABLE state are also allowed in AUTHENTICATION state. Non-protected memory pages that do not require AUTHENTICATED state can still be accessed in AUTHENTICATED state. AUTHENTICATED state is exited with either HLTA or AUTHENTICATE command. Upon reception of HLTA command, MIFARE Ultralight AES transits to the HALT state. Similarly MIFARE Ultralight AES transits to the TRACEABLE/ACTIVE state after successful 3-pass mutual authentication using the AUTHENTICATE command with [UIDRetrKey] or [OriginalityKey] respectively.

Any other unsupported data received when the device is in this state is interpreted as an error. Depending on its previous state MIFARE Ultralight AES returns to either the IDLE state or HALT state.

Authentication sequence is described in section Section 8.6.1.

8.5 Memory organization

The EEPROM memory is organized in pages with 4 bytes per page. MIFARE Ultralight AES has 60 pages in total with a user memory size of 144 byte . The memory organization is shown in Table 6 .

Table 6. Memory organization [144-byte user memory]

Page address		Byte number				Elements
Decimal	Hex	0	1	2	3	
0	00h	serial number				Manufacturer Data and Lock byte 0 and 1
1	01h	serial number				
2	02h	serial number	internal	lock byte	lock byte	
3	03h	OTP	OTP	OTP	OTP	32-bit user programmable OTP area
4	04h	user memory				User memory
5	05h					
...	...					
38	26h					
39	27h					

Table 6. Memory organization [144-byte user memory]*...continued*

Page address		Byte number				Elements
Decimal	Hex	0	1	2	3	
40	28h	lock byte	lock byte	lock byte	*RFU*	Lock byte 2, 3 and 4
41	29h	CFG_0				Configuration pages
42	2Ah	CFG_1				
...	...	RFU				
45	2Dh	LOCK_KEYS				Configuration page
...	...	RFU				
48 to 51	30h to 33h	AES authentication key [DataProtKey]				Data Protection key
52 to 55	34h to 37h	AES authentication key [UIDRetrKey]				UID retrieval key
56 to 59	38h to 3Bh	RFU				

The structure of the Manufacturer Data, Lock Bytes, OTP area and user memory pages are compatible to the existing MIFARE Ultralight portfolio.

8.5.1 UID/serial number

The 7-byte Unique IDentifier (UID) and its two check bytes (BCC) are programmed into the first 9 bytes of memory-covering page addresses 00h, 01h and the first byte of page 02h. The second byte of page address 02h is reserved for internal data. Both, UID and internal data bytes are programmed and write protected in the production test.

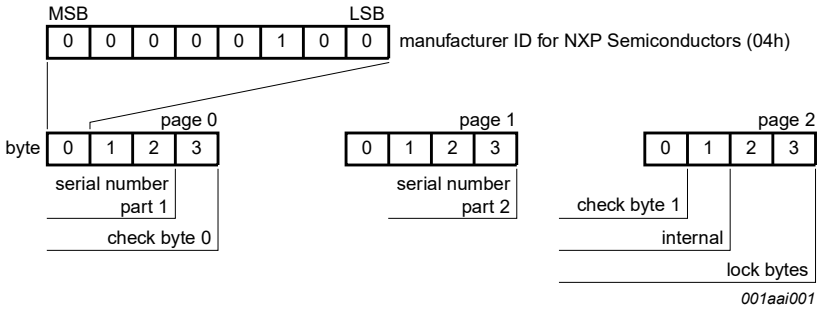


Figure 5. 7B UID/serial number

According to ISO/IEC14443-3, BCC0 is defined as CT ⊕ SN0 ⊕ SN1 ⊕ SN2. Abbreviations CT stays for Cascade Tag byte (88h). BCC1 is defined as SN3 ⊕ SN4 ⊕ SN5 ⊕ SN6. SN0 holds the Manufacturer ID for NXP Semiconductors (04h) in accordance with ISO/ IEC 14443-3.

8.5.2 Random ID

The MIFARE Ultralight AES optionally supports Random ID (RID) according to ISO 14443-3 to increase privacy of card holder. If Random ID is enabled the dedicated 128-bit AES key must be known to authenticate into TRACEABLE (UIDRetrKey) or AUTHENTICATED (DataProtKey) state to retrieve the real 7-byte UID.

The MIFARE Ultralight AES allows to switch from the 7-byte UID to the Random ID or vice versa as long as the user configuration element LOCK_USR_CFG is not set and the product is in TRACEABLE or AUTHENTICATED state. The single size 4-byte Random ID is calculated with Block Check Character (BCC) byte according to ISO/IEC 14443-3 Type A standard, see [2].

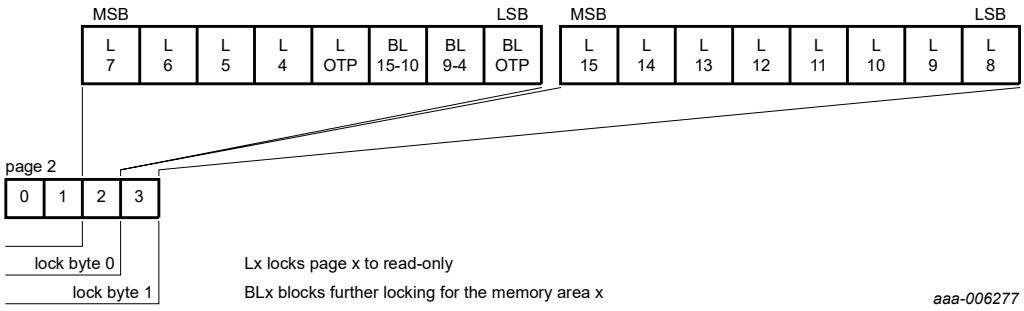
Once Random ID is activated, then the activation parameters (ATQA and SAK) are automatically adjusted accordingly. To get new Random ID, the state transition from POWER-OFF state to IDLE state is required.

Remark: MIFARE Ultralight AES in ACTIVE state with Random ID enabled, answers on a READ or FAST_READ with zeros instead of the 7-byte UID from the page 00h, 01h and 02h. Similarly READ_SIG command answer in ACTIVE state is masked with zeros. In order to reveal real UID bytes and originality signature PICC needs to be in TRACEABLE or AUTHENTICATED state.

8.5.3 Lock byte 0 and 1

Bits of byte 2 and byte 3 of page 02h represent the field programmable permanent read-only locking mechanism. Each page from 03h (OTP) to 0Fh can be individually locked by setting the corresponding locking bit Lx to logic 1 to prevent further write access. After locking, the corresponding page becomes read-only memory.

The three least significant bits of lock byte 0 are the block-locking bits. Bit 2 deals with pages 0Ah to 0Fh, bit 1 deals with pages 04h to 09h and bit 0 deals with page 03h (OTP). Once the block-locking bits are set, the locking configuration for the corresponding memory area is frozen. The functionality of the bits inside the lock bytes 0 and 1 are shown in Figure 6.



Remark: Page numbers in the figure are represented in decimal.

Figure 6. Lock bytes 0 and 1

For example if BL15-10 is set to logic 1, then bits L15 to L10 (lock byte 1, bit[7:2]) are locked. A WRITE command to page 02h, sets the locking and block-locking bits. Byte 2 and byte 3 of the WRITE command, and the contents of the lock bytes are bit-wise OR'ed and the result then becomes the new content of the lock bytes. This process can be applied once, by setting the bit to logic 1. Therefore, before writing the lock bytes, the user has to ensure that the corresponding user memory area and/or configuration bytes are correctly written.

The content of bytes 0 and 1 of page 02h is unaffected by the corresponding data bytes of the WRITE command.

The default value of the lock bytes is 00 00h.

Any write operation to the lock bytes is anti-tearing supported.

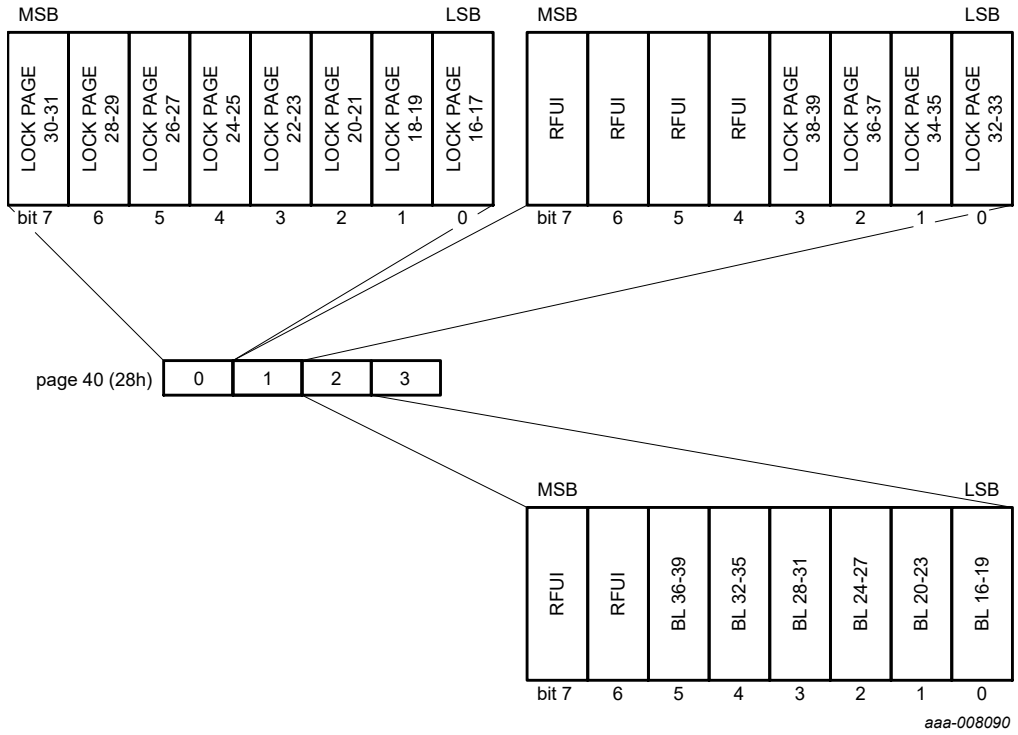
Remark: Setting a lock bit to 1 immediately prevents write access to the respective page.

For compatibility reasons, the first 96 bits of the memory area have the same functionality including static lock bits. The mapping of single lock bits to memory area for the first 96 bits is shown in Figure 6.

8.5.4 Lock byte 2, 3 and 4

To lock pages of MIFARE Ultralight AES starting at page address 10h and onwards, lock bytes 2, 3 and 4 located in page 28h (byte 0, 1 and 2) are used. Those three lock bytes cover the memory area of 96 data bytes. The granularity is 2 pages. Setting the bit to logic 1 of the lock bytes at page 28h can be applied once. The functionality of the bits inside the lock bytes 2, 3 and 4 is shown in Figure 7.

Remark: It is recommended to set all bits marked with RFU to logic "0", when writing to the lock bytes.



Remark: Page numbers in the figure are represented in decimal.

Figure 7. Lock bytes 2, 3 and 4

The default value of the lock bytes is 00 00 00h.

The value of MSB from page 28h is always 00h when read.

Any write operation to the lock bytes is anti-tearing supported.

8.5.5 OTP bytes

Page 03h is the One-Time-Programmable (OTP) page. These bytes can be bit-wise modified using the WRITE command.

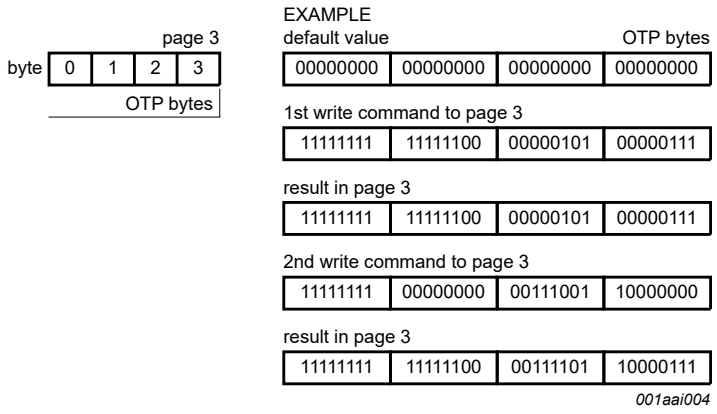


Figure 8. OTP bytes

The data bytes of the WRITE command and the current contents of the OTP bytes are bit-wise OR'ed. The result is the new OTP byte contents. If an OTP bit is set to "1", it cannot be any longer erased.

The default value of the OTP bytes is 00 00 00 00h.

Any write operation to the OTP bytes features anti-tearing support.

8.5.6 Data pages

Pages 04h to 27h for the MIFARE Ultralight AES are the user memory read/write area, referring to 144 bytes of data memory.

The access to a part of the user memory area can be restricted using an AES authentication with a key length of 128-bit, see Section 8.6.1 for further details.

Remark: The default content of the data blocks at delivery is not defined.

8.5.7 Configuration pages - 144 byte user memory

Pages 29h to 3Bh for MIFARE Ultralight AES are used to configure the user memory protection, Random ID, Counter #2 access rights, Virtual Card Type Identifier, Failed authentication limit, secure messaging and to store AES keys. The memory content of the configuration pages is defined in Table 7.

Table 7. Configuration Pages

Page Address		Byte number			
Dec	Hex	0	1	2	3
41	29h	RID_ACT / SEC_ MSG_ACT			AUTH0
42	2Ah	CNT	VCTID	AUTH_LIM0	AUTH_LIM1
43	2Bh	-			
44	2Ch	-			
45	2Dh	LOCK_KEYS	-	-	-
46	2Eh	-			
47	2Fh	-			
48	30h	AES_KEY0 [DataProtKey]			
49	31h				
50	32h				
51	33h				
52	34h	AES_KEY1 [UIDRetrKey]			
53	35h				
54	36h				
55	37h				
56	38h	-			
57	39h	-			
58	3Ah	*RFU*			
59	3Bh	*RFU*			

Table 8. Random ID RID_ACT and Secure Messaging SEC_MSG_ACT - configuration byte

Bit number							
7	6	5	4	3	2	1	0
-	-	-	-	-	-	SEC_ MSG_ACT	RID_ACT

Table 9. User memory protection AUTH0 - configuration byte

Bit number							
7	6	5	4	3	2	1	0
-	AUTH0	AUTH0	AUTH0	AUTH0	AUTH0	AUTH0	AUTH0

Table 10. Counter CNT - configuration byte

Bit number							
7	6	5	4	3	2	1	0
PROT	LOCK_ USER_CFG	-	-	CNT_ INC_EN	CNT_RD_EN	-	-

Table 11. Virtual Card Type IDentifier VCTID - configuration byte

Bit number							
7	6	5	4	3	2	1	0
VCTID	VCTID	VCTID	VCTID	VCTID	VCTID	VCTID	VCTID

Table 12. Negative authentication limit AUTH_LIM0 - configuration byte

Bit number							
7	6	5	4	3	2	1	0
AUTH_ LIM [7]	AUTH_ LIM [6]	AUTH_ LIM [5]	AUTH_LIM [4]	AUTH_ LIM [3]	AUTH_ LIM [2]	AUTH_ LIM [1]	AUTH_ LIM [0]

Table 13. Negative authentication limit AUTH_LIM1 - configuration byte

Bit number							
7	6	5	4	3	2	1	0
-	-	-	-	-	-	AUTH_ LIM [9]	AUTH_ LIM [8]

Table 14. Lock keys LOCK_Keys configuration byte

Bit number							
7	6	5	4	3	2	1	0
LOCK_ AES_KEY1	LOCK_ AES_KEY0	BLOCK_ LOCK_KEY	-	-	-	-	-

Table 15. Configuration parameter descriptions

Field	Bit(s)	Default value	Description
RID_ACT	1	0b	Enables or disables the RandomID functionality. 0b ... RandomID disabled (default) 1b ... RandomID enabled To activate RID new power-on cycle is needed.
AUTH0	7	3Ch	AUTH0 defines the page address from which the AES authentication is required. Valid address range for byte AUTH0 is from 00h to 3Bh. If AUTH0 is set to a page address outside of the valid address range, the AES authentication protection is effectively disabled.
PROT	1	1b	Configures the data access restrictions without authentication 0b … write access restricted, but read access allowed 1b … read and write access restricted
CNT_INC_EN	1	1b	Configuration option to allow a counter increment of counter "0x02" in ACTIVE or TRACEABLE state 0b … Counter increment allowed only in AUTHENTICATE state 1b … Counter increment allowed on top of AUTHENTICATE also in ACTIVE or TRACEABLE state
CNT_RD_EN	1	1b	Configuration option to read of counter "0x02" in ACTIVE or TRACEABLE state 0b ... Counter read allowed only in AUTHENTICATE state 1b ... Counter read allowed on top of AUTHENTICATE also in ACTIVE or TRA CEABLE state
VCTID	8	00000101b	Supports the virtual card architecture by replying to a Virtual Card Select Last (VCSL) command with defined Virtual Card Type IDentifier (VCTID) answer. 00000101b ... 05h (default)
AUTH_LIM	10	000h	Limitation of failed AES authentications 000h ... limit of failed AES authentication attempts disabled (default) 001h - 3FEh ... up to 1022 negative AES authentication attempts allowed
LOCK_AES_ KEY0	1	0b	LOCK_AES_KEY0 permanently locks the AES_KEY0 in pages 30h-33h. 0b … AES_KEY0 is not locked 1b … AES_KEY0 is locked **Remark:** Bit can only be set once. There is no command to set it back to unlocked.
LOCK_AES_ KEY1	1	0b	LOCK_AES_KEY1 permanently locks the AES_KEY1 in blocks 34h-37h. 0b ... AES_KEY1 is not locked 1b ... AES_KEY1 is locked **Remark:** Bit can only be set once. There is no command to set it back to unlocked.
BLOCK_LOCK_ KEY	1	0b	BLOCK_LOCK_KEY permanently locks the LOCK_AES_KEY0 and LOCK_AES_ KEY1.

Table 15. Configuration parameter descriptions...*continued*

Field	Bit(s)	Default value	Description
			0b ... not locked 1b ... locked **Remark:** Bit can only be set once. There is no command to set it back to unlocked.
LOCK_USR_CFG	1	0b	LOCK_USR_CFG permanently locks the modification of user configuration elements. 0b … not locked 1b … locked **Remark:** Bit can only be set once. There is no command to set it back to unlocked.
SEC_MSG_ACT	1	0b	SEC_MSG_ACT allows the user to activate Secure Messaging. 0b … Secure messaging not activated (default) 1b … Secure messaging activated
RFU	-	not defined	Reserved for Future Use - implemented. The recommendation is to write bits and bytes denoted as RFU as 0b.

Remark: LOCK_USR_CFG, LOCK_AES_KEY1, LOCK_AES_KEY0, BLOCK_LOCK_KEY bits activate the permanent write protection of the corresponding configuration memory sections. If write protection is enabled, each write attempt leads to locked memory elements immediately to a NAK response.

8.5.8 Configuration for memory access via AES authentication

The start of authentication protected memory segment is configured with the configuration byte AUTH0, located in page 29h within byte 3, see Section 8.5.7 .

- AUTH0 defines the page address from which the authentication is required. Valid address values for byte AUTH0 are from 00h to 3Bh.
- Setting AUTH0 to a value higher than 3Bh effectively disables memory protection.
- PROT configuration bit only determines in ACTIVE or TRACEABLE state if write access is restricted or both read and write access are restricted.
- To activate new AUTH0 and PROT setting, the state transition from POWER-OFF state to IDLE state is required.

8.5.9 Counter 3x 24-bit one way

The MIFARE Ultralight AES features three independent 24-bit one-way counters with two of them accessible without restrictions in ACTIVE and TRACEABLE states and third one with optional increment and read control in those states. Settings of the counter with the optional AES protection are configurable within the user memory protection configuration. These counters are located in a separate part of the EEPROM which is not directly addressable using READ, FAST_READ or WRITE commands. The actual value can be retrieved by using the READ_CNT command, the counters can be incremented with the INCR_CNT command. The INCR_CNT command features anti-tearing support.

In the initial state, counter values are set to 000000h. The maximum value of each counter is FFFFFFh.

The counters can be incremented by an arbitrary 3-byte value. The incremented value is valid immediately without necessity of an RF reset or re-activation. Once counter value reaches FFFFFFh and an increment is performed via a valid INCR_CNT command, the MIFARE Ultralight AES replies a NAK. If the sum of the addressed counter value and the increment value in the INCR_CNT command is higher than FFFFFFh, the MIFARE Ultralight AES replies a NAK and does not update the respective counter.

An increment by zero (000000h) is always possible, but does not have any impact on the counter value.

Remark: With the user memory protection configuration (see Section 8.5.7) the read and increment functionality of the counter "0x02" can be restricted.

8.6 AES authentication protection

The memory access to a configurable part of the memory can be constrained by a 3-pass mutual authentication. The 128-bit secret AES key is typically programmed into the configuration pages at the tag personalization in a secure environment.

In the initial state of MIFARE Ultralight AES, the authentication protection is disabled. The AES key is freely writable in this state. Access to the configuration pages and any part of the user memory can be restricted by setting AUTH0 to a page address within the available memory space. From this page address onwards the memory is protected, see Section 8.5.8.

Once AES authentication protection is activated, following items must be handled appropriately:

- AUTH0 defines the page address from which the authentication is required. Valid address values for byte AUTH0 are from 00h to 3Bh. Value higher than 3Bh effectively disables memory protection, but still keeping AES authentication procedure working.
- AUTH_LIM to limit failed AES authentication attempts during lifetime
- PROT determines if write access is restricted or both read and write accesses are restricted
- CNT_RD_EN to limit read of counter "0x02" in ACTIVE and TRACEABLE state. If set, Read allowed in AUTHENTICATED state only.
- CNT_INC_EN to limit increment of counter "0x02" in ACTIVE and TRACEABLE state. If set, Increment allowed in AUTHENTICATED state only.

8.6.1 AES authentication

The AES authentication implemented in the MIFARE Ultralight AES proves that two entities hold the same secret and each entity can be seen as a reliable partner for onwards communication. The 3-pass authentication using the authenticate command is outlined in Table 16 by following the byte order for AES computations. The Initialization Vector (IV) for encryption of the response uses a byte value of all zeroes.

Table 16. AES authentication

PCD	Data exchanged	PICC
The reader device is always the entity which starts an authentication procedure. This is done by sending an authenticate command. As parameter, the key number is passed to the PICC in order to select a certain key stored in its non-volatile memory.	→ AUTHENTICATE *(KeyNo)*	
	← *E(Kx,RndB)*	The PICC generates a random challenge *RndB*. This random number is enciphered with the selected key *Kx*.
The PCD deciphers the received message and retrieves *RndB*. (The used key for the deciphering obviously has to be the same as for the previous enciphering by the PICC.) The *RndB* is rotated left by 8 bits, yielding *RndB'*. The PCD itself generates a random challenge *RndA*. The PCD enciphers this *RndA* concatenated with the rotated *RndB'* using the selected key *Kx*.	→ *E(Kx,RndA||RndB')*	

Table 16. AES authentication*...continued*

PCD	Data exchanged	PICC
	← *E(Kx, RndA')*	The PICC deciphers the received message and retrieves *RndA* and *RndB'*. The PICC now verifies the sent *RndB* by comparing it against the received *RndB'* after rotating the original *RndB* left by 8 bits. A successful verification proves to the PICC that the PICC and the PCD possess the same secret key. If the verification fails, the PICC stops the authentication procedure and returns a NAK. In case of successful execution, the PICC enters either AUTHENTICATE or TRACEABLE state depending on key number used as argument in the first AUTHENTICATE command. The *RndA* is rotated left by 8 bits, yielding *RndA'* which is enciphered again by the PICC. Enciphered message is answered to PCD.
The PCD deciphers the received message and retrieves *RndA'*. The PCD now verifies the sent *RndA* by comparing it against the received *RndA'* after rotating the original *RndA* left by 8 bits. A successful verification proves to the PCD that the PICC and the PCD possess the same secret key. If the verification fails, the PCD exits the authentication procedure and may halt the PICC. In case of successful execution, the PCD enters the relevant authentication state and proceeds further accordingly.		

The cryptographic method is based on AES in Cipher-Block chaining (CBC) mode according to NIST Special Publication 800-38A. The used key is a 128-bit AES Key.

Remark: To reduce the risk on card-only side channel attack to the AES keys, a failed authentication limit (AUTH_LIM) can be set.

8.6.2 AES authentication example

A numerical example of a AES authentication process is shown below in Table 17. The default 128-bit AES key used has a value of all zeros.

Table 17. Numerical AES authentication example

#	PCD	Data exchanged	PICC
1	start the authentication procedure	→ **1A**	
2		← **AF**D5A847B84862FF38 74A7F07B8DDF351B	generate RndB=1AE4174CA173EBBC 59165CEBE2F20821 IV=00000000000000000000000000000000 ek(Kx, RndB)=D5A847B84862FF38 74A7F07B8DDF351B
3	decipher ek(RndB) to retrieve RndB	→	

Table 17. Numerical AES authentication example*...continued*

#	PCD	Data exchanged	PICC
	generate RndA=F29B0123F5C00DF6 12487BBF42468C7E IV=00000000000000000000000000000000 ek(RndA || RndB')=CDF22C5F7A92F0AF 0155612B9B236AC7A424BC52 38D41AD041B8165B7D99E524	**AF**CDF22C5F7A92F0 AF 0155612B9B236AC7A4 24BC5238D41AD041B8 165B7D99E524	
4		← **00**2C743D6B1E128F80 76BD197B76012CE8	decipher ek(RndA || RndB') to retrieve RndA ek(Kx, RndA')=2C743D6B1E128F80 76BD197B76012CE8 RndA'=9B0123F5C00DF612 487BBF42468C7EF2 IV = 00000000000000000000000000000000
5	decipher and verify ek(RndA')		

8.6.3 Programming of the AES key to memory

The 16 bytes of the AES [DataProtKey] are programmed to memory pages from 30h to 33h . Keys themselves can be written during personalization or at any later stage in a secure environment, as long as the key is not locked for update in the user configuration segment. AES [UIDRetrKey] is stored in memory addresses from 34h until 37h. In case keys are not locked, MIFARE Ultralight AES allows to change AES-keys without authentication as long as AUTH0 is not set to a page address before or at page address where keys bytes are stored. Otherwise MIFARE Ultralight AES requires to be in the AUTHENTICATED state to allow to write AES keys.

Table 18. DataProtKey memory configuration

Page address	Byte Number			
Hex	Byte 0	Byte 1	Byte 2	Byte 3
30h	K0	K1	K2	K3
31h	K4	K5	K6	K7
32h	K8	K9	K10	K11
33h	K12	K13	K14	K15

On example of AES key 0 = 000102030405060708090A0B0C0D0E0Fh, the command sequence needed for key programming with WRITE command is:

- A2 30 0F 0E 0D 0C CRC
- A2 31 0B 0A 09 08 CRC
- A2 32 07 06 05 04 CRC
- A2 33 03 02 01 00 CRC

The memory content after those WRITE commands is shown in the table below:

Table 19. DataProtKey memory configuration based on example configuration

Page address		Byte Number			
Dec	Hex	Byte 0	Byte 1	Byte 2	Byte 3
64	30h	0Fh	0Eh	0Dh	0Ch
65	31h	0Bh	0Ah	09h	08h

Table 19. DataProtKey memory configuration based on example configuration*...continued*

Page address		Byte Number			
Dec	Hex	Byte 0	Byte 1	Byte 2	Byte 3
66	32h	07h	06h	05h	04h
67	33h	03h	02h	01h	00h

The memory pages holding an AES key can never be directly read, independent of the configuration.

Remark: A re-programmed AES authentication key has immediate effect.

8.6.4 Protection of configuration pages

The configuration pages are from the access point of view seen as user memory and can be protected by the 3-pass mutual authentication as well. In the same way as for user memory, the protection level is defined with the PROT bit to restrict access. The protection is enabled by setting the AUTH0 byte to a value that is within the addressable memory space.

8.6.5 Limiting failed authentication attempts

To reduce the risk that the 128-bit AES key leaks due to side-channel attacks, the maximum allowed number of negative authentication attempts can be set using AUTH_LIM by a 10 bits configuration element. This mechanism is disabled by setting AUTH_LIM to a value of 000h, which is also the default state of MIFARE Ultralight AES.

If AUTH_LIM is not equal to 000h, each failed authentication is internally counted and stored. The count operation features anti-tearing support. As soon as the internal counter reaches the number specified in AUTH_LIM, any further failed authentication attempt leads to a permanent lock of the protected part of the user memory for the specified access rights. Specifically, each subsequent authentication fails independent if the authentication is valid or not.

Any successful authentication, before reaching the limit of failed authentication attempts, decrements the internal counter value by 10h. In case the counter is at a value of 10h or below the counter is reset.

8.7 Plain communication

The command and response data is not secured. The data is sent in plain over the RF interface.

8.8 CMAC protected message integrity protection

MIFARE Ultralight AES offers the option to enable secure messaging for message integrity protection following NIST Special Publication 800-38B, see [15]. Once AES authentication protection is activated, secure messaging mode can be enabled by setting SEC_MSG_ACT. It enables CMAC protected message integrity protection. Prior to data transmission, a 3-pass mutual authentication needs to be done between PICC and PCD which results in the generation of session key used in the secure messaging, see Section 8.8.1.

8.8.1 Session Key Generation

The session key is a temporary key created after a successful authentication and it will be valid only for the given session, see Figure 9.

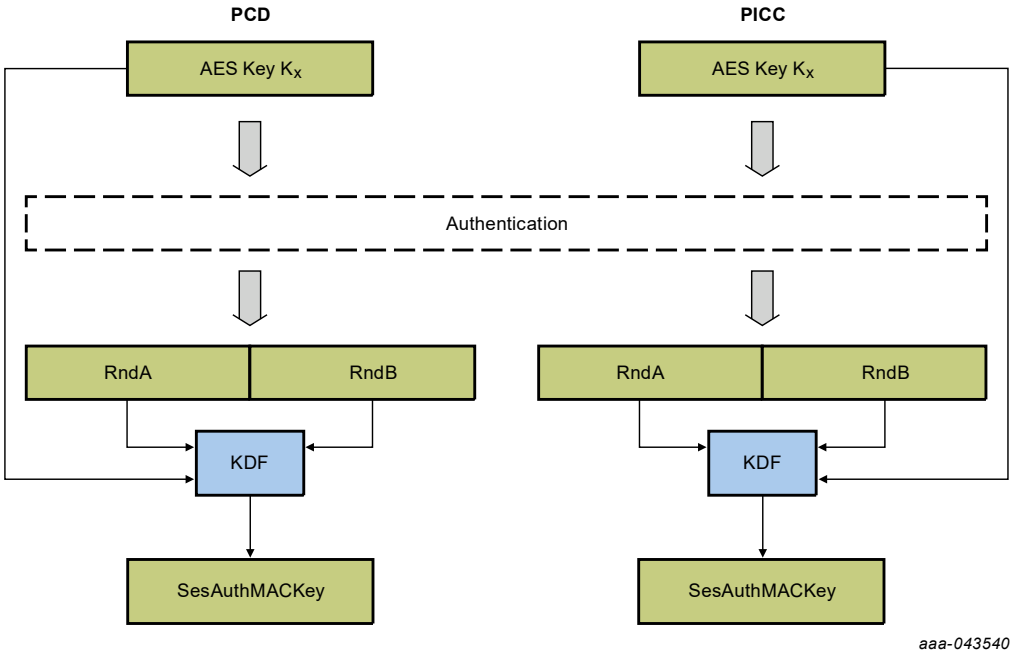


Figure 9. Session key generation for Secure Messaging

Session key generation is according to NIST Special Publication 800-108 in counter mode, see [17].

The KDF (Key Derivation Function) is the Pseudo Random Function (PRF) applied during the key generation is the CMAC algorithm described in NIST Special Publication 800-38B, see [15]. The key derivation key is the key Kx that was applied during authentication. The generated key is also an AES 128-bit key.

Note that NIST SP 800-108 allows defining a different order than proposed by the standard as long as it is unambiguously defined. The input data is constructed using the following fields:

- a 2-byte label, distinguishing the purpose of the key: 5AA5h for MACing
- a 2-byte counter, fixed to 0001h as only 128-bit keys are generated.
- a 2-byte length, fixed to 0080h as only 128-bit keys are generated.
- a 26-byte context, constructed using the two random numbers exchanged, RndA and RndB

With that input data specification, the 32-byte input session vector SV_2 is derived as follows:

SV_2 = *5Ah||A5h||00h||01h||00h||80h||RndA[15..14]|| RndA[13..8] XOR RndB[15..10])||RndB[9..0]||RndA[7..0]*

with || indicating concatenation operator.

Then, the 16-byte session key is constructed as follows:

SesAuthMACKey = PRF(K_x; SV_2)

8.8.2 CMAC Calculation for data integrity

The Cipher-based Message Authentication Codes (CMAC) are calculated using the underlying block cipher according to the CMAC standard described in NIST Special. Publication 800-38B, see [15]. Padding is applied according to the standard.

8.8.3 CMAC Communication Mode

PCD communicating with MIFARE Ultralight AES in MAC communication mode shall calculate MAC over:

- 2-bytes of Command Counter - CmdCtr

- 1- byte of Command Code
- Argument bytes

For responses, the MIFARE Ultralight AES calculates CMAC over:

- 2-bytes of Command Counter - CmdCtr
- Response data bytes

CRC bytes appended in both directions at the end of the communication message are excluded from the MAC calculation. CmdCtr is included in the CMAC calculation for commands and responses in order to prevent replay attacks. The CmdCtr is reset to 0000h at PCD and PICC after a subsequent authentication using AUTHENTICATE command. CmdCtr value is maintained as long as MIFARE Ultralight AES remains in AUTHENTICATED/TRACEABLE state. Subsequent authentications using the AUTHENTICATE command will reset CmdCtr to 0000h. The command counter is incremented between each command and response.

In cryptographic calculations, the CmdCtr is represented with LSB first. If the CmdCtr holds the value FFFFh and a command maintaining the active authentication arrives at the PICC, it leads to an error response and the command is handled like the CMAC was wrong. If a CMAC over the command is received, the PICC verifies the CMAC and rejects commands that do not contain a valid CMAC. In this case, the ongoing command and transaction are aborted, the authentication state is lost and the NAK is sent without a CMAC appended. Note that any other error during the command execution has the same consequences.

In MAC communication mode ACK responses are replaced by standalone MAC calculated over CmdCtr. In this case also CRC is added.

8.9 Product originality

The MIFARE Ultralight AES offers two ways to verify the originality of the IC manufactured by NXP Semiconductors:

- For NXP tools AES-based originality key leveraging the AES authentication with an NXP die specific 128-bit AES key stored in the hidden part of the memory to check the origin of the IC
- For customer application ECC (Elliptic Curve Cryptography) based originality signature according to ECDSA (Elliptic Curve Digital Signature Algorithm) with a public key for verification

The purpose of the ECC originality check during (pre-)personalization is to protect customer investments by identifying mass penetration of non-NXP originated MIFARE Ultralight AES ICs into an infrastructure. As individual signatures can still be copied, it does not completely prevent hardware copy or emulation of individual MIFARE Ultralight AES ICs. As such, a valid signature is not a full guarantee. Therefore, this signature validation should be complemented with a check to detect if multiple ICs with the same UID are being introduced in the system.

The 48-bytes asymmetric originality signature is based on standard Elliptic Curve Cryptography (ECC curve secp192r1, see [19]), according to the ECDSA algorithm and only requires a public key for the verification. The originality signature can be read with the READ_SIG command. The MIFARE Ultralight AES provides the possibility to customize the originality signature to personalize the IC individually for specific application.

If the PICC is not configured for Random ID, the READ_SIG command is available even in ACTIVE state. If the PICC is configured for Random ID, an authentication with either DataProdKey or UIDRetrKey is required, see Section 8.5.

8.9.1 Originality Signature

At delivery, the MIFARE Ultralight AES is pre-programmed with the NXP originality signature. This signature is locked in the hidden part of the memory. If needed, the signature can be re-programmed with a custom-specific signature using the WRITE_SIG command during the personalization process by the customer. The signature can be permanently locked afterward with the LOCK_SIG command to avoid further modifications.

Remark: If no customized originality signature is required, it is recommended to permanently lock the NXP signature during the initialization process with the LOCK_SIG command.

8.9.2 Originality Signature at Delivery

To verify the signature (for example with the use of the public domain crypto library OpenSSL) the tool domain parameters shall be set to secp192r1, defined within the standards for elliptic curve cryptography SEC, see [19]. As input data for signature validation the 7-byte UID without Hash is in use.

For details on how to check the NXP signature values are provided in following application note see [5].

8.10 Virtual Card Architecture Support

The MIFARE Ultralight AES supports in ACTIVE state the Virtual Card Architecture by replying to a Virtual Card Select Last (VCSL) command with a Virtual Card Type IDentifier (VCTID), see Section 10.11. The VCTID that is replied can be programmed in the configuration pages. It enables infrastructure support of this feature to process MIFARE product-based cards across different MIFARE families in a common way.

For example, a contactless system is enabled to select a specific virtual MIFARE product-based card inside a cell phone. It can use the same card identification principle to detect that the MIFARE Ultralight AES belongs to the system, see Section 10.11.

9 Command overview

The MIFARE Ultralight AES card activation follows part 3 of ISO/IEC 14443 Type A, see [2]. After the MIFARE Ultralight AES has been selected, it can either be deactivated using the HLTA command, or MIFARE Ultralight AES commands (e.g. READ or WRITE) can be performed.

9.1 MIFARE Ultralight AES Command Overview

All non ISO/IEC 14443-3 commands for the MIFARE Ultralight AES are shown in Table 20. All memory access commands are transmitted in either plain or CMAC protected compliant to the CMAC mode of NIST Special Publication 800-38B, see [15].

Table 20. Command overview

Command	ISO/IEC 14443	Command code (hexadecimal)
Request	REQA	26h (7 bit)
Wake-up	WUPA	52h (7 bit)
Anti-collision CL1	Anti-collision CL1	93h 20h
Select CL1	Select CL1	93h 70h
Anti-collision CL2	Anti-collision CL2	95h 20h
Select CL2	Select CL2	95h 70h
HALT	HLTA	50h 00h
READ	-	30h
WRITE	-	A2h
FAST_READ	-	3Ah
GET_VERSION	-	60h
READ_SIG	-	3Ch
WRITE_SIG	-	A9h
LOCK_SIG	-	ACh
READ_CNT	-	39h
INC_CNT	-	A5h
AUTHENTICATE - Part 1	-	1Ah
AUTHENTICATE - Part 2	-	AFh
VCSL	-	4Bh

Remark: All commands use the coding and framing as described in [2], if not otherwise specified.

9.2 Timings

The timing shown in this document is not to scale and values are rounded to 1 µs.

All given command and response transmission times refer to the data frames including start of communication and end of communication. A PCD data frame contains the start of communication (1 "start bit") and the end of communication (one logic 0 + 1 bit length of unmodulated carrier). A PICC data frame contains the start of communication (1 "start bit") and the end of communication (1 bit length of no subcarrier).

The command response time is specified according to [2] as an integer n which specifies the PCD to PICC frame delay time. The Frame Delay Time (FDT) from PICC to PCD is at least 87 µs which corresponds to n=9. The maximum command response time is specified as a timeout value.

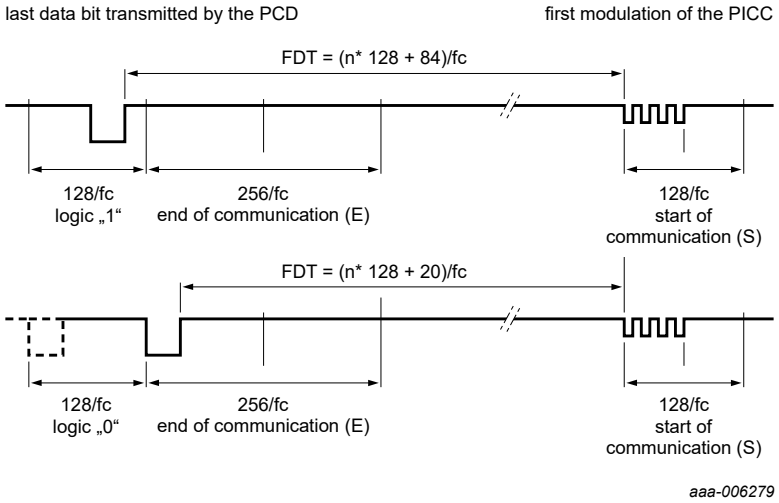


Figure 10. Frame Delay Time (from PCD to PICC)

Remark: Due to the coding of commands, the measured timings usually exclude (a part of) the end of communication. Consider this factor when comparing the specified with the measured times.

9.3 ACK and NAK

The MIFARE Ultralight AES uses, apart from the responses defined in the following sections, two half-byte answers to acknowledge the command received in ACTIVE, TRACEABLE and AUTHENTICATED state abbreviated as ACK for positive acknowledge and NAK for negative acknowledge. Valid values for ACK and NAK are shown in Table 21.

Table 21. ACK and NAK values

Answer value Code 4-bit	Answer explanation ACK/NAK
Ah	Acknowledge (ACK)
0h	NAK for invalid argument (i.e. invalid page address)
1h	NAK for parity or CRC error
4h	NAK for a counter overflow
5h	NAK for EEPROM write error
6h	NAK if valid page indicators are corrupted for the given tearing supported pages.
7h	NAK for EEPROM write error

After every NAK, the MIFARE Ultralight AES performs unselect and returns to IDLE or HALT state.

9.4 ATQA and SAK responses

For details on the Type Identification Procedure, refer to the AppNote [3]. The MIFARE Ultralight AES replies to a REQA or WUPA command with the ATQA value shown in Table 22. It replies to final Select command with the SAK value shown in Table 22. The 2-byte ATQA value is transmitted with the least significant byte first.

Remark: The ATQA coding in bits 7 and 8 indicate the UID size according to ISO/IEC 14443 independent from the settings of the UID usage.

Remark: The bit numbering in the ISO/IEC 14443 starts with LSB = bit 1 and not with LSB = bit 0. So 1 byte counts bit 1 to bit 8 instead of bit 0 to 7.

9.5 Summary of device identification data

For more details on the values below, please refer to [2], [3] and [4].

Table 22. Summary of relevant data for device identification

Code	Length	Value	Binary Format	Remark
ATQA	2 Byte	0044h	0000 0000 0100 0100	In case of double size UID
ATQA	2 Byte	0000h	0000 0000 0000 0000	In case of RID enabled
CT	1 Byte	88h	1000 1000	Cascade Tag, ensures collision with cascade level 1 products Cascade Tag is not applicable in case RID enabled
SAK	1 Byte	04h	0000 0100	Indicates additional cascade level in case of double size UID
SAK	1 Byte	00h	0000 0000	In case of double size UID or cascade level 1 in case of RID
Manufacturer Byte	1 Byte	04h	0000 0100	Indicates NXP Semiconductors as manufacturer in case of double size UID
Random ID Indicator	1 Byte	08h	0000 1000	In case of Random ID 1st byte (08h) indicates RID itself

10 MIFARE Ultralight AES - Commands

In the following subsections, CMACs are displayed as optional fields on commands and responses. If SEC_MSG_ACT is enabled, then the CMAC bytes are present. If SEC_MSG_ACT is disabled, then the CMAC bytes are not present.

10.1 GET_VERSION

The GET_VERSION command is used to retrieve information on the MIFARE family, product version, storage size and other product data required to identify the MIFARE Ultralight AES.

This command is also available on other MIFARE products to have a common way of identifying products across platforms and evolution steps.

The GET_VERSION command has no arguments and replies the version information for the specific MIFARE Ultralight AES type. The command structure is shown in Figure 11 and Table 23 the response description is shown in Table 24.

Table 26 shows the required timing.

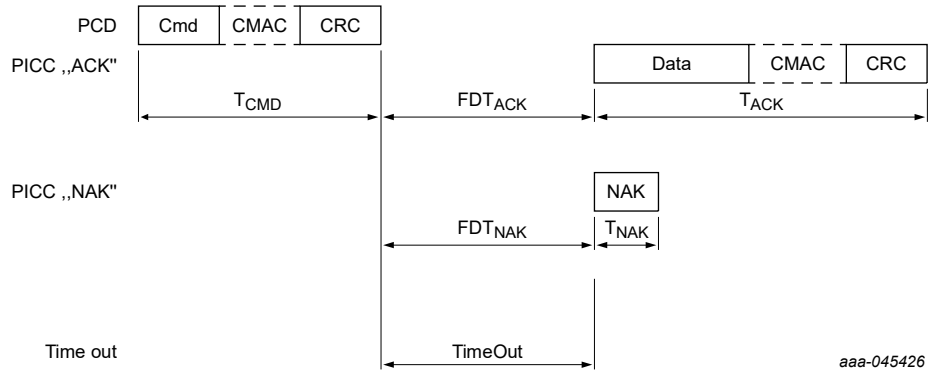


Figure 11. GET_VERSION command

Table 23. GET_VERSION command

Name	Code	Description	Length
Cmd	60h	Get product version	1 byte
[CMAC]	-	Optional: If secure messaging is enabled by set of SEC_MSG_ACT	[8 bytes]
CRC	-	CRC according to [2]	2 bytes

Table 24. GET_VERSION response

Name	Code	Description	Length
Data	-	Product version information (see Table 25)	8 bytes
[CMAC]	-	Optional: If secure messaging is enabled by set of SEC_MSG_ACT	[8 bytes]
CRC	-	CRC according to [2]	2 bytes
NAK	see Table 21	see Section 9.3	4-bits

Table 25. GET_VERSION data response for MIFARE Ultralight AES

Byte no.	Description	MIFARE Ultralight AES	Interpretation
0	fixed header	00h	
1	vendor ID	04h	NXP Semiconductors
2	product type	03h	MIFARE Ultralight
3	product subtype	01h / 02h	17 pF / 50 pF
4	major product version	04h	AES
5	minor product version	00h	V0
6	storage size	0Fh	144-byte
7	protocol type	03h	ISO/IEC 14443-3 compliant

Table 26. GET_VERSION timing

These times exclude the end of communication of the PCD.

	Without secure messaging	With secure messaging
FDT_{ACK} min	n=9 [1]	
FDT_{ACK} max	$T_{TimeOut}$	
$FDT_{NAK\ min}$	n=9	
$FDT_{NAK\ max}$	$T_{TimeOut}$	
TimeOut	5 ms	
T_{CMD}	283 µs	963 µs
T_{ACK}	868 µs	1549 µs
T_{NAK}	57 µs	

[1] Refer to Section 9.2

10.2 READ

The READ command requires a start page address, and returns the 16 bytes of four pages. For example, if address (Addr) is 03h then pages 03h, 04h, 05h, 06h are returned. So called roll-over mechanism (described later) applies if the READ command address is near the end of the accessible memory area. Same mechanism applies if at least part of the addressed pages is within an authentication protected area. For details the command structure, refer to Figure 12.

Table 29 shows the required timing.

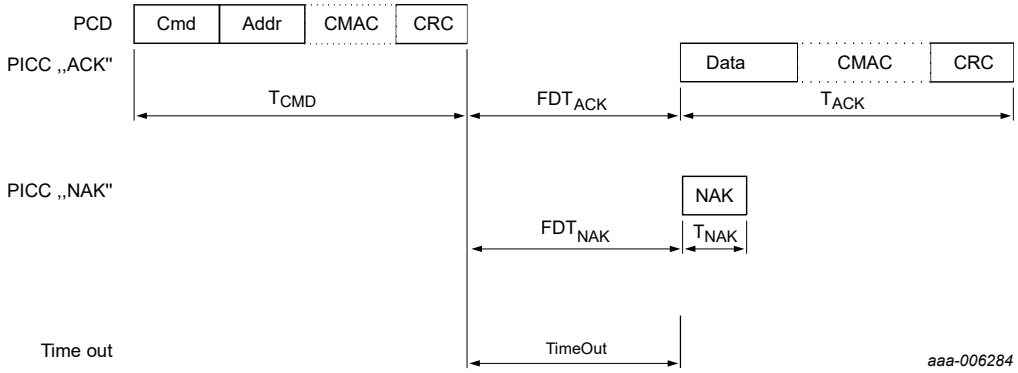


Figure 12. READ

Table 27. READ command

Name	Code	Description	Length
Cmd	30h	read four pages	1 byte
Addr	-	start page address	1 byte
[CMAC]	-	Optional: If secure messaging is enabled by set of SEC_MSG_ACT	[8 bytes]
CRC	-	CRC according to [2]	2 bytes

Table 28. READ response

Name	Code	Description	Length
Data	-	data content of the addressed pages	16 bytes
[CMAC]	-	Optional: If secure messaging is enabled by set of SEC_MSG_ACT	[8 bytes]
CRC	-	CRC according to [2]	2 bytes
NAK	see Table 21	see Section 9.3	4-bits

Table 29. READ timing

These times exclude the end of communication of the PCD.

	Without secure messaging	With secure messaging
FDT_{ACK} min	n=9 [1]	
FDT_{ACK} max	$T_{TimeOut}$	
$FDT_{NAK\ min}$	n=9	
$FDT_{NAK\ max}$	$T_{TimeOut}$	
TimeOut	5 ms	
T_{CMD}	368 µs	1048 µs
T_{ACK}	1548 µs	2228 µs
T_{NAK}	57 µs	

[1] Refer to Section 9.2

In the default state of MIFARE Ultralight AES, all memory pages in the range from 00h to 3Bh are allowed as Addr parameter to the READ command.

Addressing a memory page above the limit results in a NAK response. A roll-over mechanism is implemented to continue reading from page 00h once the end of the accessible memory is reached if at least first addressed page is within allowed limit.

The following conditions apply if part of the memory is authentication protected for read access:

- if MIFARE Ultralight AES is in the ACTIVE or TRACEABLE state

- addressing a page which is equal to or higher than AUTH0 results in a NAK response

- addressing a page lower than AUTH0 results in data being returned with the roll-over mechanism occurring just before the AUTH0 defined page

- in TRACEABLE state if secure messaging enabled, a CMAC on the READ command is required

- if MIFARE Ultralight AES is in the AUTHENTICATED state

- the READ command behaves like on a MIFARE Ultralight AES without access protection

- if secure messaging enabled, a CMAC on the READ command is required

Remark: AES key values can never be directly read out of the memory. When reading from the pages holding key values, all 00h bytes are replied to the PCD instead.

10.3 FAST_READ

The FAST_READ command requires a start page address and an end page address and returns bytes of addressed pages. For example if the start address is 03h and the end address is 07h then pages 03h, 04h, 05h, 06h, and 07h are returned. If either start or end address is outside accessible area, then MIFARE Ultralight AES replies with a NAK. For details on command structure, refer to Figure 13.

Table 32 shows the required timing.

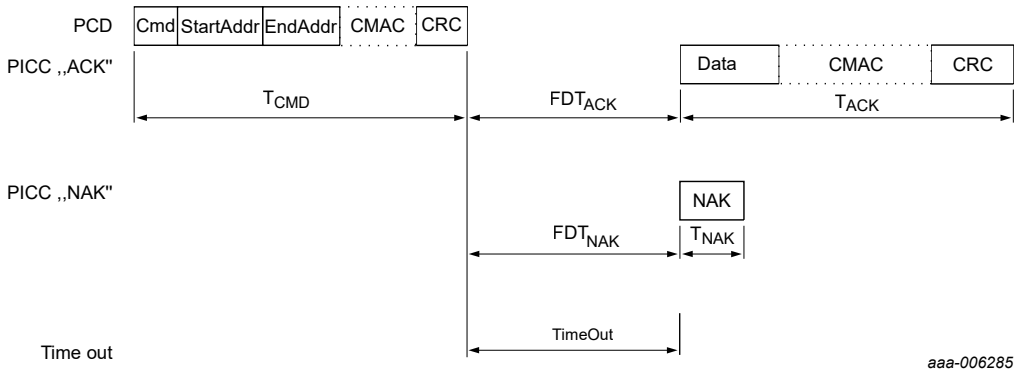


Figure 13. FAST_READ command

Table 30. FAST_READ command

Name	Code	Description	Length
Cmd	3Ah	read multiple pages	1 byte
StartAddr	-	start page address	1 byte
EndAddr	-	end page address	1 byte
[CMAC]	-	Optional: If secure messaging is enabled by set of SEC_MSG_ACT	[8 bytes]
CRC	-	CRC according to [2]	2 bytes

Table 31. FAST_READ response

Name	Code	Description	Length
Data	-	data content of the addressed pages	(EndAddr - StartAddr + 1) *4 bytes
[CMAC]	-	Optional: If secure messaging is enabled by set of SEC_MSG_ACT	[8 bytes]
CRC	-	CRC according to [2]	2 bytes
NAK	see Table 21	see Section 9.3	4-bit

Table 32. FAST_READ timing

These times exclude the end of communication of the PCD.

	Without secure messaging	With secure messaging
FDT_{ACK} min	n=9 [1]	
FDT_{ACK} max	$T_{TimeOut}$	
$FDT_{NAK\ min}$	n=9	
$FDT_{NAK\ max}$	$T_{TimeOut}$	
TimeOut	5 ms	
T_{CMD}	453 µs	1133 µs
T_{ACK}	depending on the number of pages read	
T_{NAK}	57 µs	

[1] Refer to Section 9.2

In the default state of the MIFARE Ultralight AES, all memory pages in the range from 00h to 3Bh are allowed as StartAddr parameter to the FAST_READ command.

Addressing a memory page above the limits results in a NAK response.

The EndAddr parameter must be equal to or higher than the StartAddr otherwise NAK response is provided.

The following conditions apply if part of the memory is access control protected for read access:

- if the MIFARE Ultralight AES is in the ACTIVE or TRACEABLE state
  - if EndAddr is equal to or higher than AUTH0 a NAK is replied
  - in TRACEABLE state if secure messaging enabled, a CMAC on the FAST_READ command is required
- if the MIFARE Ultralight AES is in the AUTHENTICATED state
  - the FAST_READ command behaves like on a MIFARE Ultralight AES without access protection
  - if secure messaging enabled, a CMAC on the FAST_READ command is required

Remark: Key values can never directly be read out of the memory. When reading from the pages holding those two values, all 00h bytes are replied to the PCD instead.

Remark: The FAST_READ command is able to read out the whole accessible memory in one shot. Nevertheless, receive buffer of the PCD must be able to handle the requested amount of data as there is no chaining possibility.

10.4 WRITE

The WRITE command requires a block address, and writes 4 bytes of data into the addressed MIFARE Ultralight AES page. The WRITE command is shown in Figure 14.

Table 35 shows the required timing.

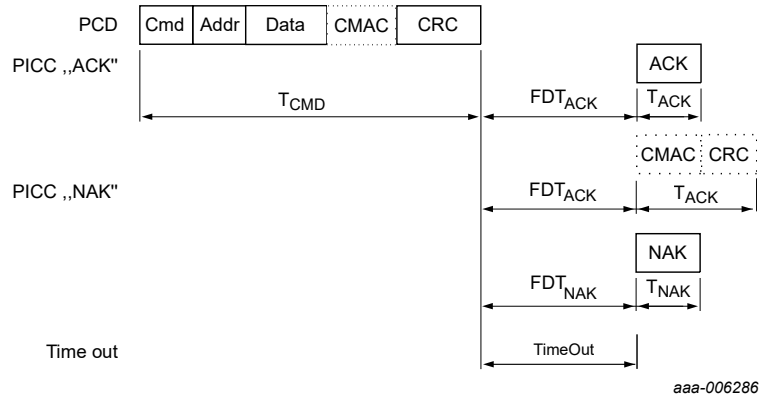


Figure 14. WRITE

Table 33. WRITE command

Name	Code	Description	Length
Cmd	A2h	write one page	1 byte
Addr	-	page address	1 byte
Data	-	data	4 bytes
[CMAC]	-	Optional: If secure messaging is enabled by set of SEC_MSG_ACT	[8 bytes]
CRC	-	CRC according to [2]	2 bytes

Table 34. WRITE response

Name	Code	Description	Length
ACK / NAK	see Table 21	see Section 9.3	4-bit
[CMAC]	-	Optional: If secure messaging is enabled by set of SEC_MSG_ACT. Note that the ACK is replaced by a MAC, calculated over just the CmdCtr, and CRC calculated over the MAC bytes.	[8 bytes]
[CRC]	-	CRC according to [2]	[2 bytes]

Table 35. WRITE timing

These times exclude the end of communication of the PCD.

	Without secure messaging	With secure messaging
FDT_{ACK} min	n=9 [1]	
FDT_{ACK} max	$T_{TimeOut}$	
$FDT_{NAK\ min}$	n=9	
$FDT_{NAK\ max}$	$T_{TimeOut}$	
TimeOut	5 ms	
T_{CMD}	708 µs	1388 µs
T_{ACK}	57 µs	869 µs
T_{NAK}	57 µs	

[1] Refer to Section 9.2

In the default state of MIFARE Ultralight AES, the pages address 02h to 3Bh are valid Addr parameters to the WRITE command.

Addressing a memory page above the limits results in a NAK response.

Pages which are locked against writing cannot be reprogrammed using WRITE command.

The following conditions apply if part of the memory is authentication protected for write access:

• if MIFARE Ultralight AES is in the ACTIVE or TRACEABLE state

- writing to a page which address is equal or higher than AUTH0 results in a NAK response

- in TRACEABLE state if secure messaging enabled, a CMAC on the WRITE command is required

• if MIFARE Ultralight AES is in the AUTHENTICATED state

- the WRITE command behaves like on a MIFARE Ultralight AES without access protection MIFARE Ultralight AES features tearing support write operations to specific memory content.

The following pages are protected against tearing events during a WRITE operation:

• page 02h containing lock bytes 0 and 1

• page 03h containing OTP bits

• page 28h containing the lock bytes 2, 3 and 4 for the MIFARE Ultralight AES

10.5 READ_CNT

The READ_CNT command is used to read out the current value of one of the 3 one-way counters of MIFARE Ultralight AES. The command has a single argument specifying the counter number and returns the 24-bit counter value of the corresponding counter. Counters are always readable, except in case of the counter "0x02" with the optional AES authentication protection enabled. In that case, the counter 0x02 is readable only in the AUTHENTICATE state. The command structure is shown in Figure 15.

Table 38 shows the required timing.

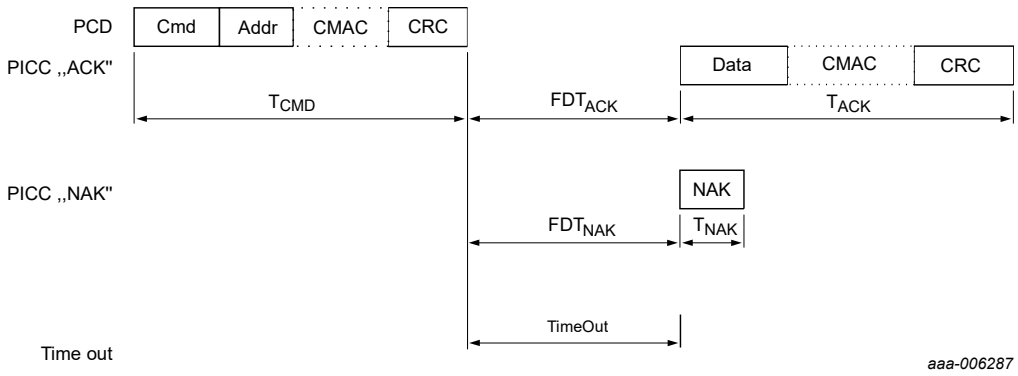


Figure 15. READ_CNT command

Table 36. READ_CNT command

Name	Code	Description	Length
Cmd	39h	read counter	1 byte
Addr	-	counter number from 00h to 02h	1 byte
[CMAC]	-	Optional: If secure messaging is enabled by set of SEC_MSG_ACT	[8 bytes]
CRC	-	CRC according to [2]	2 bytes

Table 37. READ_CNT response

Name	Code	Description	Length
Data	-	counter value	3 bytes
[CMAC]	-	Optional: If secure messaging is enabled by set of SEC_MSG_ACT	[8 bytes]
CRC	-	CRC according to [2]	2 bytes
NAK	see Table 21	see Section 9.3	4-bit

Table 38. READ_CNT timing

These times exclude the end of communication of the PCD.

	Without secure messaging	With secure messaging
FDT_{ACK} min	n=9 [1]	
FDT_{ACK} max	$T_{TimeOut}$	
$FDT_{NAK\ min}$	n=9	
$FDT_{NAK\ max}$	$T_{TimeOut}$	
TimeOut	5 ms	
T_{CMD}	368 µs	1048 µs
T_{ACK}	444 µs	1124 µs
T_{NAK}	57 µs	

[1] Refer to Section 9.2

If secure messaging enabled, a CMAC on the READ_CNT command is required.

10.6 INCR_CNT

The INCR_CNT command is used to increment one of the 3x one-way counters of the MIFARE Ultralight AES. Two arguments are the counter number and the increment value. Counters are always incrementable, except in case of the counter "0x02" with the optional AES authentication protection enabled. In that case, the counter 0x02 can be incremented only in the AUTHENTICATE state. The INCR_CNT command is shown in Figure 16.

Table 41 shows the required timing.

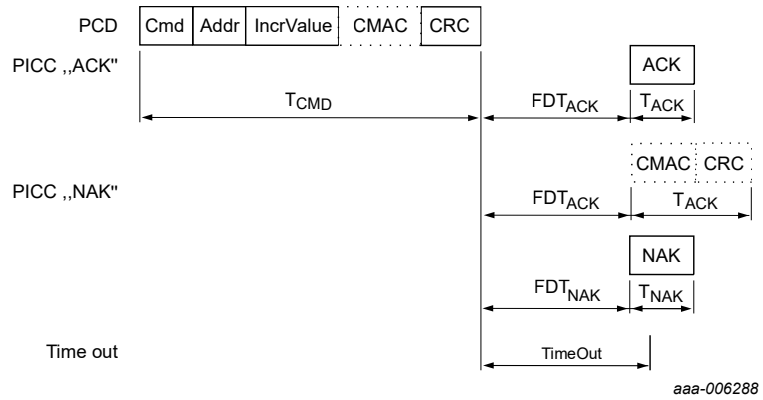


Figure 16. INCR_CNT command

Table 39. INCR_CNT command

Name	Code	Description	Length
Cmd	A5h	increment counter	1 byte
Addr	-	counter number from 00h to 02h	1 byte
IncrValue	-	increment value, only the 3 least significant bytes are relevant	4 byte
[CMAC]	-	Optional: If secure messaging is enabled by set of SEC_MSG_ACT	[8 bytes]
CRC	-	CRC according to [2]	2 bytes

Table 40. INCR_CNT response

Name	Code	Description	Length
ACK	see Table 21	see Section 9.3	4-bit
[CMAC]	-	Optional: If secure messaging is enabled by set of SEC_MSG_ACT. Note that the ACK is replaced by a MAC, calculated over just the CmdCtr, and CRC calculated over the MAC bytes.	[8 bytes]
[CRC]	-	CRC according to [2]	[2 bytes]
NAK	see Table 21	see Section 9.3	4-bit

Table 41. INCR_CNT timing

These times exclude the end of communication of the PCD.

	Without secure messaging	With secure messaging
FDT_{ACK} min	n=9 [1]	
FDT_{ACK} max	$T_{TimeOut}$	
$FDT_{NAK\ min}$	n=9	
$FDT_{NAK\ max}$	$T_{TimeOut}$	
TimeOut	5 ms	
T_{CMD}	708 µs	1388 µs
T_{ACK}	57 µs	869 µs
T_{NAK}	57 µs	

[1] Refer to Section 9.2

The increment value argument is a 4-byte field to support the same command structure as the WRITE command. As the counter width is only 3 byte, the last transmitted, most significant byte is ignored.

Any increment value is allowed. The final counter value is FFFFFFh. No further increment is possible after the final value is reached. Also, trying to increment the current value by a number which would exceed the final value leads to a NAK response and the counter remains unchanged. An increment by 0 is allowed and leaves the counter unchanged.

The order of bytes in the increment argument follows the same order that the bytes are sent via the communication interface. This means from the LSB (IncrValue0) to MSB (IncValue3), where the last valid byte is actually IncrValue2. As an example, an increment of the counter 00h by 01h, is formulated as INCR CNT 00 01 00 00 00.

If secure messaging enabled, a CMAC on the INCR_CNT command is required.

10.7 READ_SIG

The READ_SIG retrieves the originality signature based on Elliptic Curve Cryptography Digital Signature Algorithm (ECDSA). The purpose of originality check signature is to protect the MIFARE Ultralight AES contactless IC from mass copying. The purpose of originality check signature is not to completely prevent HW copy or emulation of individual ICs. A public key is required for the verification, which is done outside the card. The NXP originality signature is computed over the UID and written during NXP manufacturing. If the PICC is not configured for Random ID, the command is available even in ACTIVE state. If the PICC is configured for Random ID, an authentication with the 128-bit AES [DataProtKey] or [UIDRetrKey] is required to enter TRACEABLE or AUTHENTICATE state.

The READ_SIG command returns an IC-specific, 48-byte ECC signature. The command structure is shown in Figure 17. The originality signature can be changed (see, Section 8.9.1) if it has been unlocked with the LOCK_SIG command (see, Section 10.9).

Table 44 shows the required timing.

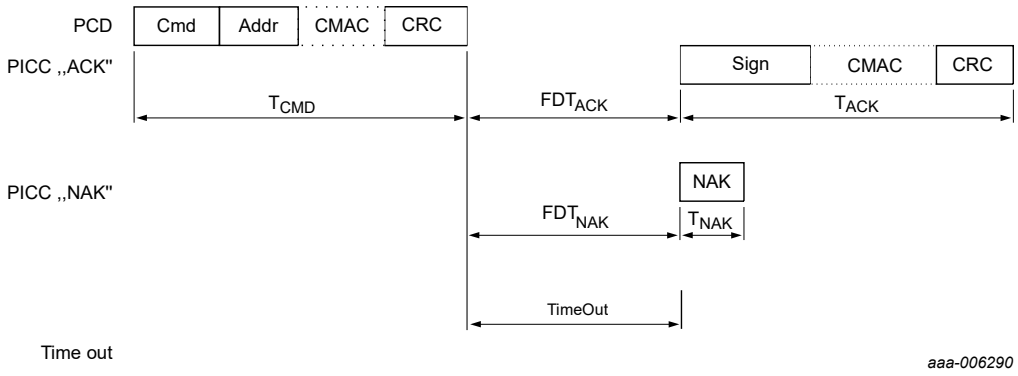


Figure 17. READ_SIG command

Table 42. READ_SIG command

Name	Code	Description	Length
Cmd	3Ch	read ECC signature	1 byte
Addr	00h	RFU, is set to 00h	1 byte
[CMAC]	-	Optional: If secure messaging is enabled by set of SEC_MSG_ACT	[8 bytes]
CRC	-	CRC according to [2]	2 bytes

Table 43. READ_SIG response

Name	Code	Description	Length
Sign	-	ECC signature	48 bytes
[CMAC]	-	Optional: If secure messaging is enabled by set of SEC_MSG_ACT	[8 bytes]
CRC	-	CRC according to [2]	2 bytes
NAK	see Table 21	see Section 9.3	4-bit

Table 44. READ_SIG timing

These times exclude the end of communication of the PCD.

	Without secure messaging	With secure messaging
FDT_{ACK} min	n=9 [1]	
FDT_{ACK} max	$T_{TimeOut}$	
$FDT_{NAK\ min}$	n=9	
$FDT_{NAK\ max}$	$T_{TimeOut}$	
TimeOut	5 ms	
T_{CMD}	368 µs	1048 µs
T_{ACK}	4266 µs	4944 µs
T_{NAK}	57 µs	

[1] Refer to Section 9.2

If secure messaging enabled, a CMAC on the READ_SIG command is required.

Remark: Details on how to check that the signature value is provided in the following Application note, [5].

10.8 WRITE_SIG

The WRITE_SIG command allows the writing of a customized originality signature into the dedicated originality signature memory.

The WRITE_SIG command requires an originality signature block address, and writes 4 bytes of data into the addressed originality signature block. The WRITE_SIG command is shown in Figure 18.

Table 47 shows the required timing.

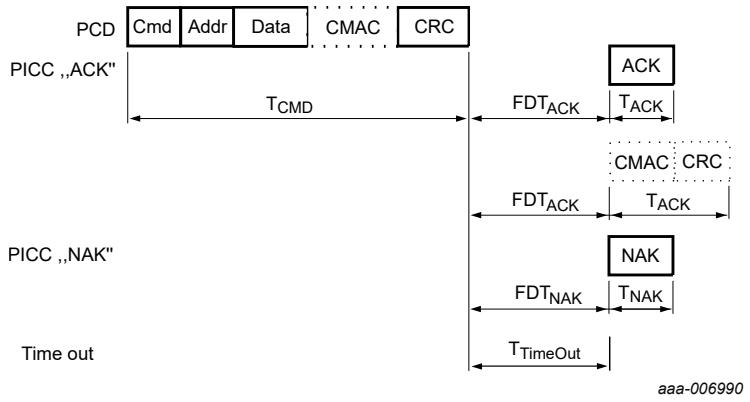


Figure 18. WRITE_SIG command

Table 45. WRITE_SIG command

Name	Code	Description	Length
Cmd	A9h	write one originality signature block	1 byte
Addr	-	block address	1 byte
Data	-	signature bytes to be written	4 bytes
[CMAC]	-	Optional: If secure messaging is enabled by set of SEC_MSG_ACT	[8 bytes]
CRC	-	CRC according to [2]	2 bytes

Table 46. WRITE_SIG response

Name	Code	Description	Length
ACK	see Table 21	see Section 9.3	4-bit
[CMAC]	-	Optional: If secure messaging is enabled by set of SEC_MSG_ACT. Note that the ACK is replaced by a MAC, calculated over just the CmdCtr, and CRC calculated over the MAC bytes.	[8 bytes]
[CRC]	-	CRC according to [2]	[2 bytes]
NAK	see Table 21	see Section 9.3	4-bit

Table 47. WRITE_SIG timing

These times exclude the end of communication of the PCD.

	Without secure messaging	With secure messaging
FDT_{ACK} min	n=9 [1]	
FDT_{ACK} max	$T_{TimeOut}$	
$FDT_{NAK\ min}$	n=9	
$FDT_{NAK\ max}$	$T_{TimeOut}$	
TimeOut	5 ms	
T_{CMD}	708 µs	1388 µs
T_{ACK}	57 µs	869 µs
T_{NAK}	57 µs	

[1] Refer to Section 9.2

In the initial state of MIFARE Ultralight AES, the following originality signature blocks 00h to 0Bh are valid Addr parameters to the WRITE_SIG command. Addressing a memory block beyond the limits above results in a NAK response from MIFARE Ultralight AES.

Table 48. Blocks for the WRITE_SIG command

Originality signature block	Byte 0	Byte 1	Byte 2	Byte 3
00h	LSByte			
...				
...				
...				
0Bh				MSByte

If the originality signature is locked or permanently locked, a WRITE_SIG command results in a NAK response from the MIFARE Ultralight AES.

If secure messaging enabled, a CMAC on the WRITE_SIG command is required.

10.9 LOCK_SIG

The LOCK_SIG command allows the user to unlock, lock or permanently lock the dedicated originality signature memory. The originality signature can only be unlocked, if the originality signature is not permanently locked. There is no command to unlock the originality signature, if the originality signature is permanently locked. The LOCK_SIG command is shown in Figure 19.

Table 51 shows the required timing.

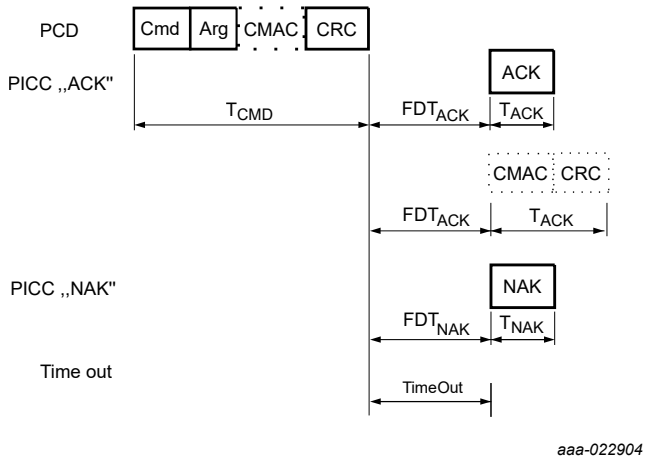


Figure 19. LOCK_SIG command

Table 49. LOCK_SIG command

Name	Code	Description	Length
Cmd	ACh	lock signature	1 byte
Arg	-	locking action	1 byte
		00h - unlock	1 byte
		01h - lock	1 byte
		02h - permanently lock	1 byte
[CMAC]	-	Optional: If secure messaging is enabled by set of SEC_MSG_ACT	[8 bytes]
CRC	-	CRC according to [2]	2 bytes

Table 50. LOCK_SIG response

Name	Code	Description	Length
ACK	see Table 21	see Section 9.3	4 bits
[CMAC]	-	Optional: If secure messaging is enabled by set of SEC_MSG_ACT. Note that the ACK is replaced by a MAC, calculated over just the CmdCtr, and CRC calculated over the MAC bytes.	[8 bytes]
[CRC]	-	CRC according to [2]	[2 bytes]

Table 50. LOCK_SIG response...*continued*

Name	Code	Description	Length
NAK	see Table 21	see Section 9.3	4 bits

Table 51. LOCK_SIG timing

These times exclude the end of communication of the PCD.

	Without secure messaging	With secure messaging
FDT_{ACK} min	n=9 [1]	
FDT_{ACK} max	$T_{TimeOut}$	
$FDT_{NAK\ min}$	n=9	
$FDT_{NAK\ max}$	$T_{TimeOut}$	
TimeOut	5 ms	
T_{CMD}	368 µs	1048 µs
T_{ACK}	57 µs	869 µs
T_{NAK}	57 µs	

[1] Refer to Section 9.2

If secure messaging enabled, a CMAC on the LOCK_SIG command is required.

Remark: If no further change of the customized originality signature is required, it is recommended to permanently lock the NXP signature during the initialization process with the LOCK_SIG command.

10.10 AUTHENTICATE

The AUTHENTICATE command is used to authenticate with a 3-pass mutual authentication the MIFARE Ultralight AES and PCD. The authentication process is detailed, in Section 8.6.2. Authentication with the defined 128-bit AES Data Protection key or UID retrieval key is required to either access the protected user memory pages or to retrieve the double size UID in case Random ID is enabled, as well as the originality signature.

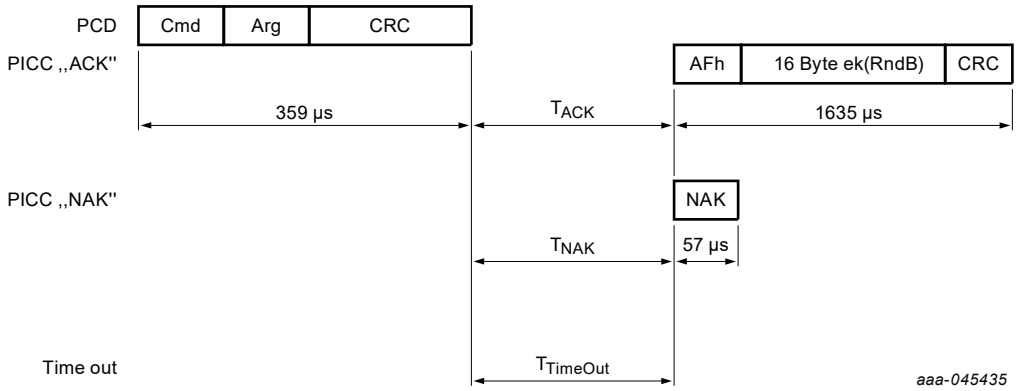


Figure 20. AUTHENTICATE Part 1

Table 52. AUTHENTICATE Part 1 command

Name	Code	Description	Length
Cmd	1Ah	authentication part 1	1 byte
Arg	00h / 01h / 02h	00h … DataProtKey 01h … UIDRetrKey 02h … OriginalityKey	1 byte
CRC	-	CRC according to [2]	2 bytes
AFh	AFh	first response byte indicates that the authentication process needs a second command part	1 byte
ek(RndB)	-	16-byte encrypted PICC random number RndB	16 bytes
NAK	see Table 21	see Section 9.3	4-bit

Table 53. AUTHENTICATE Part 1 response

Name	Code	Description	Length
AFh	AFh	first response byte indicates that the authentication process needs a second command part	1 byte
ek(RndB)	-	16-byte encrypted PICC random number RndB	16 bytes
CRC	-	CRC according to [2]	2 bytes
NAK	see Table 21	see Section 9.3	4-bit

Table 54. AUTHENTICATE Part 1 timing

These times exclude the end of communication of the PCD.

	T_{ACK} min	T_{ACK} max	T_{NAK} min	T_{NAK} max	$T_{TimeOut}$
AUTHENTICATE part 1	n=9 [1]	$T_{TimeOut}$	n=9	$T_{TimeOut}$	5 ms

[1] Refers to Section 9.2

Table 55. AUTHENTICATE Part 2

Code	Parameter	Data	Integrity mechanism	Response
AFh	-	ek(RndA+RndB')	Parity, CRC	'00' + ek(RndA')

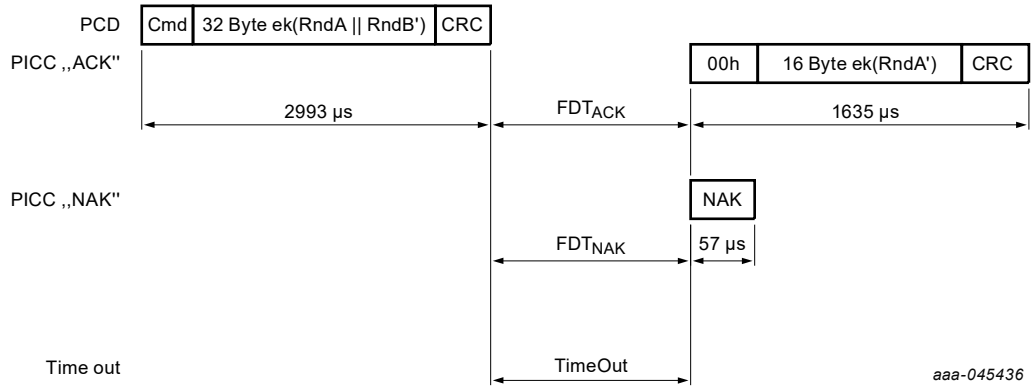


Figure 21. AUTHENTICATE Part 2

Table 56. AUTHENTICATE Part 2 command

Name	Code	Description	Length
Cmd	AFh	fixed first byte for the AUTHENTICATE part 2 command	1 byte
ek(RndA || RndB')	-	32-byte encrypted random numbers RNDA concatenated with RndB'	32 bytes
CRC	-	CRC according to [2]	2 bytes

Table 57. AUTHENTICATE Part 2 response

Name	Code	Description	Length
00h	00h	first response byte indicates that the authentication process is finished after this command	1 byte
ek(RndA')	-	16-byte encrypted, shifted PCD random number RndA'	16 bytes
CRC	-	CRC according to [2]	2 bytes
NAK	see Table 21	see Section 9.3	4-bit

Table 58. AUTHENTICATE Part 2 timing

These times exclude the end of communication of the PCD.

	T_{ACK} min	T_{ACK} max	T_{NAK} min	T_{NAK} max	$T_{TimeOut}$
AUTHENTICATE part 2	n=9 [1]	$T_{TimeOut}$	n=9	$T_{TimeOut}$	5 ms

[1] Refers to Section 9.2

10.11 VCSL

The VCSL command is used to enable a unique identification and selection process across different physical MIFARE product-based cards and virtual MIFARE implementations. The command requires a 16-byte installation identifier IID and a 4-byte PCD capability value as parameters. The parameters are present to support compatibility to other MIFARE product-based devices, but are not used or checked inside the MIFARE Ultralight AES.

Nevertheless, the number of bytes is checked for correctness. The answer to the VCSL command is the VCTID value stored in the user configuration segment. This identifier indicates the type of card or ticket. Using this information, the contactless reader can decide whether the ticket belongs to the installation or not. The command structure is shown in Figure 22 and Table 59.

Table 61 shows the required timing.

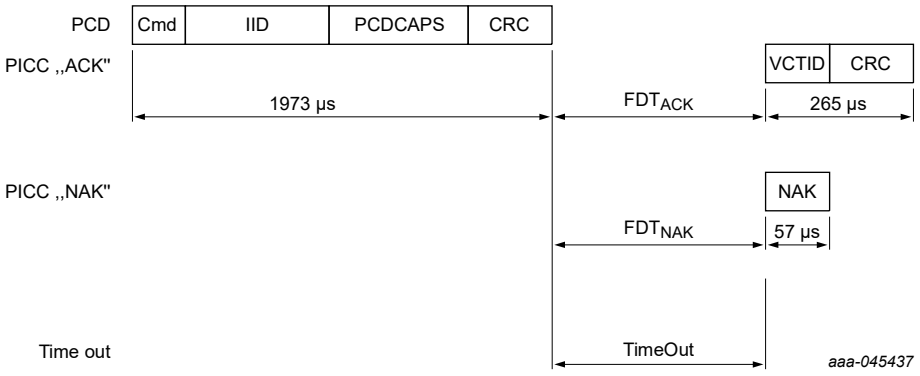


Figure 22. VCSL command

Table 59. VCSL command

Name	Code	Description	Length
Cmd	4B	Virtual Card Select Last command	1 byte
IID	-	installation identifier	16 bytes
PCDCAPS	-	PCD capabilities	4 bytes
CRC	-	CRC according to [1]	2 bytes

Table 60. VCSL command

Name	Code	Description	Length
VCTID	-	Virtual Card Type Identifier	1 byte
CRC	-	CRC according to [2]	2 bytes
NAK	see Table 21	see Section 9.3	4-bit

Table 61. VCSL timing

These times exclude the end of communication of the PCD.

	T_{ACK} min	T_{ACK} max	T_{NAK} min	T_{NAK} max	$T_{TimeOut}$
VCSL	n=9 [1]	$T_{TimeOut}$	n=9	$T_{TimeOut}$	5 ms

[1] Refers to Section 9.2

11 Limiting values

Stresses exceeding one or more of the limiting values, can cause permanent damage to the device. Exposure to limiting values for extended periods can affect device reliability.

Table 62. Limiting values

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

Symbol	Parameter	Condition	Min	Max	Unit
$P_{d,max}$	maximum power dissipation		-	120	mW
$I_{LA-LB,max}$	maximum input current		-	40	mA
T_{stg}	storage temperature		-55	+125	°C
T_{amb}	ambient temperature		-25	+70	°C
V_{ESD}	electrostatic discharge voltage on LA/LB	[1]	-	2	kV

[1] ANSI/ESDA/JEDEC JS-001; Human body model: C = 100 pF, R = 1.5 kΩ

Remark: Stress above one or more of the limiting values may cause permanent damage to the device. Exposure to limiting values for extended periods may affect device reliability.

CAUTION

This device has limited built-in ElectroStatic Discharge (ESD) protection. The leads should be shorted together or the device placed in conductive foam during storage or handling to prevent electrostatic damage to the gates.

12 Characteristics

12.1 Electrical characteristics

Table 63. Characteristics of MIFARE Ultralight AES

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
f_i	input frequency		-	13.56	-	MHz
C_i	MF0AESxy input capacitance [1]	T_{amb} = 22 °C	-	17	-	pF
	MF0AESHxy input capacitance [1]	T_{amb} = 22 °C	-	50	-	pF
EEPROM characteristics						
t_{ret}	retention time	T_{amb} = 22 °C	10	-	-	year
$N_{endu(W)}$	write endurance	T_{amb} = 22 °C	100000	-	-	cycle

[1] f_i = 13.56 MHz; 2 V RMS

13 Wafer specification

Table 64. Wafer specifications MIFARE Ultralight AES

Wafer	
diameter	200 mm typical (8 inches)
maximum diameter after foil expansion	210 mm
die separation process	laser dicing
thickness	120 µm ± 15 µm | 75 µm ± 10 µm
flatness	not applicable
Potential Good Dies per Wafer (PGDW)	42521
Wafer backside	
material	Si
treatment	ground and stress relieve
roughness	R_a max = 0.5 µm
	R_t max = 5 µm
Chip dimensions	
step size[1]	x = 832 µm
	y = 832 µm
gap between chips[1]	typical = 20 µm
	minimum = 5 µm
Passivation	
type	sandwich structure
material	PSG / nitride
thickness	500 nm / 600 nm
Au bump (substrate connected to VSS)	
material	> 99.9 % pure Au
hardness	35 to 80 HV 0.005
shear strength	> 70 MPa
height	18 µm
height uniformity	within a die = ±2 µm
	within a wafer = ±3 µm
	wafer to wafer = ±4 µm
flatness	minimum = ±1.5 µm
size	LA, LB, VSS, TP [2] = 80 µm × 80 µm
size variation	±5 µm
under bump metallization	sputtered TiW

[1] The step size and the gap between chips may vary due to changing foil expansion
[2] Pads VSS and TESTIO are disconnected at wafer treatment.

14 Delivery

The customer purchasing a product of the MIFARE Ultralight AES family has to make sure that they receive the evaluated version. This section describes the measures that are needed to ensure delivery of the evaluated version.

The evaluated version of the MIFARE Ultralight AES can be ordered from NXP by referencing the respective commercial type name as listed in Section 5.

NXP offers two ways of delivery of the product:

1. The customer collects the product themselves at the NXP site.
2. The product is sent by NXP to the customer and protected by special measures.

These methods are described in the Section 14.1 and Section 14.2 respectively.

14.1 Delivery as a wafer

When the product is delivered as wafer, there reside functional and non-functional ICs on the wafer. The non-functional ICs cannot be used but have to be handled securely, too. These ICs must be destroyed to such an extent that no analysis or misuse is possible after destruction. The non-functional ICs (scrap) shall be handled secure until the destruction.

Information about non-functional items is accessible via the eMAP-Portal (http://wmt.nxp.com). The Access sheet with the Login data is enclosed with the delivery to allow the download of the electronic wafer map file. In this case, the information about non-functional ICs is stored in a so-called wafer map file. The electronic wafer map file covers the electrical test results and additionally the results of mechanical/visual inspection.

14.2 Delivery as a module

When the product is delivered as module, there reside functional and non-functional modules on the reel. The non-functional modules cannot be used but have to be handled securely, too. These modules must be destroyed to such an extent that no analysis or misuse is possible after destruction.

The non-functional modules (scrap) shall be handled secure until the destruction. Information about non-functional items is accessible via the eMAP-Portal (http:// wmt.nxp.com). The Access sheet with the Login data is enclosed with the delivery to allow the download of the file. In this case, the information about non-functional modules is stored in a so-called SNR file.

14.3 Delivery method one: The customer collects the product themselves

The customer fetches the product from the following location:

NXP Semiconductors (Thailand)

303 Chaengwattana Rd.Laksi

Bangkok

10210 Thailand

This method guarantees that the customer gets authentic products.

14.4 Delivery method two: The product is sent by NXP and protected by special measures

To guarantee that the product is not manipulated during the delivery, NXP has defined three security measures:

1. The product is delivered in parcels sealed with special tapes. The customer can examine these tapes in order to make sure that they have not been manipulated.
2. The customer shall identify the product as described in Section 10.1.
3. The customer should check the originality by verification of the Originality Signature Section 8.9.2.

These measures shall be applied to ensure that a genuine chip is in use. The product is delivered directly to the customer or via the Global Distribution Center:

NXP Semiconductors Netherlands B.V.

(Global Distribution Centre)

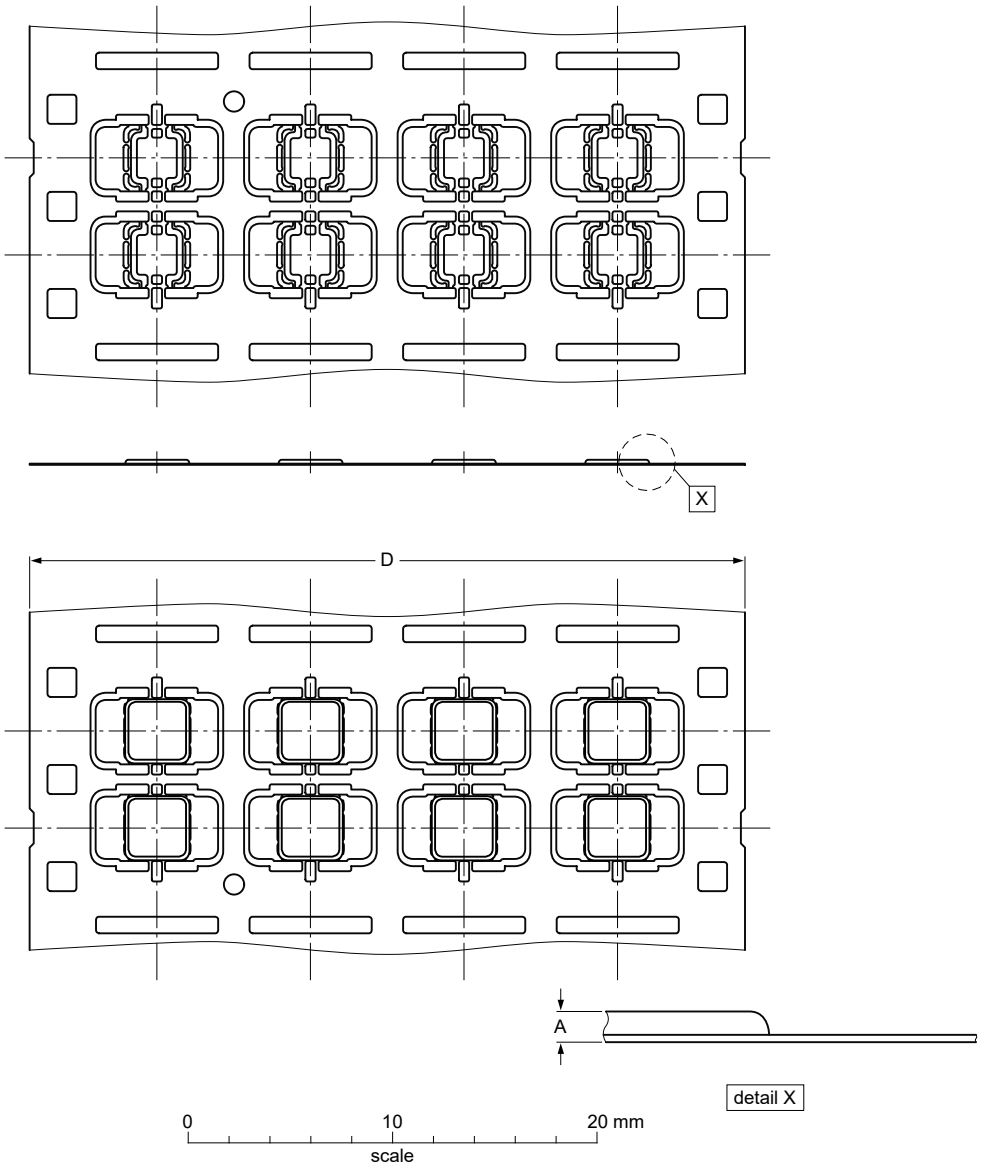
c/o CEVA Logistics (Malaysia) Sdn Bhd

Lot 9A Jalan Tiang U8/92, Bukit Jelutong Industrial Park, 40150 Shah Alam, Selangor Darul Ehsan, MALAYSIA

15 Package outline

For more details on the MOA8 contactless modules, please refer to [12].

PLLMC: plastic leadless module carrier package; 35 mm wide tape **SOT500-4**



Dimensions

Unit		$A^{(1)}$	D
mm	max	0.26	35.05
	nom		35.00
	min		34.95

For unspecified dimensions see PLLMC-drawing given in the subpackage code.

Note
1. Total package thickness, exclusive punching burr.

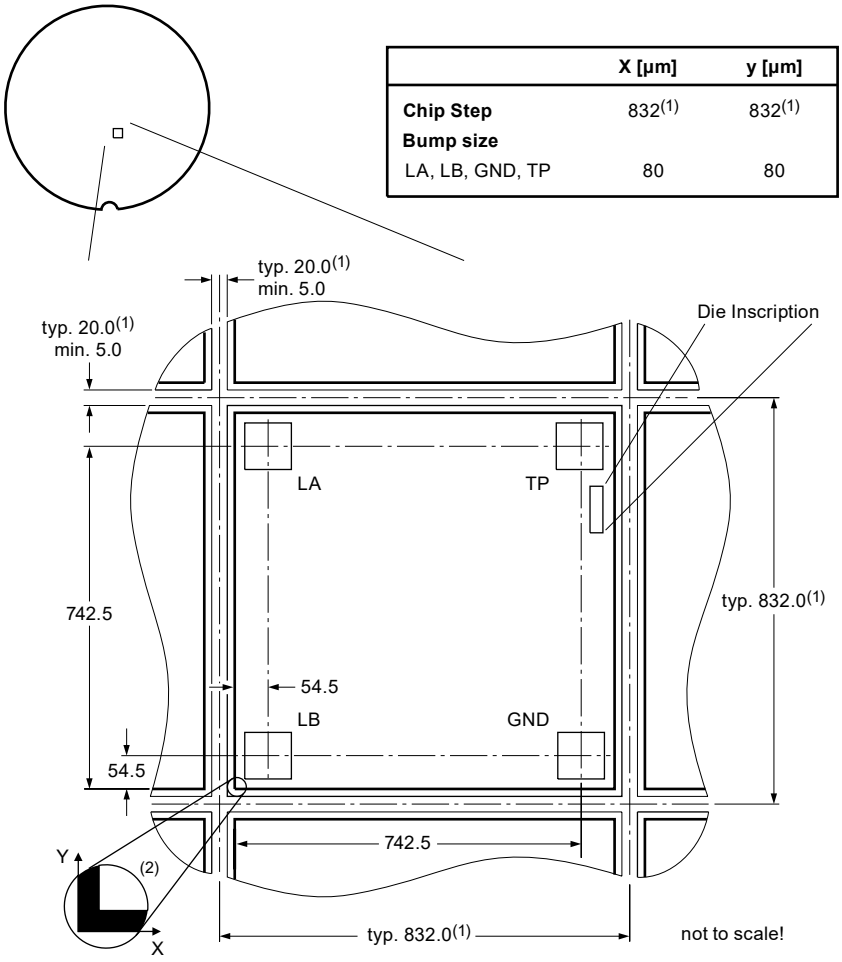
sot500-4_po

Outline version	References				European projection	Issue date
	IEC	JEDEC	JEITA			
SOT500-4	- - -	- - -	- - -			11-02-18

Figure 23. Package outline SOT500-4

15.1 Bare die outline

For more details on the wafer delivery forms, see [13].



(1) the air gap and thus the step size may vary due to varying foil expansion
(2) all dimensions in µm, pad locations measured from metal ring edge (see detail)

aaa-045439

Figure 24. Bare die outline

16 Abbreviations

Table 65. Abbreviations

Acronym	Description
AES	Advanced Encryption Standard
ACK	Positive Acknowledge
ATQA	Answer To ReQuest, type A
BCC	Block Check Characters byte
CBC	Cipher-Block Chaining
CRC	Cyclic Redundancy Check
CT	Cascade Tag, Type A
EEPROM	Electrically Erasable Programmable Read-Only Memory
fc	carrier frequency 13.56 MHz
FFC	Film Frame Carrier
HLTA	Halt A command
IC	Integrated Circuit
IV	Initialization Vector
LSB	Least Significant Bit
CMAC	Cipher-based Message Authentication Codes
MSB	Most Significant Bit
NAK	Negative AcKnowledge
NVM	Non-Volatile Memory
OTP	One Time Programmable
Passive ACK	Implicit acknowledge without PICC answer
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Card
POR	Power On Reset
REQA	ReQuest Answer, type A
RF	Radio Frequency
SAK	Select AcKnowledge, type A
UID	Unique IDentifier
WUPA	Wake-UP command, type A

17 References

[1] **ISO/IEC 14443-2: July 2016**

Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 2: Radio frequency power and signal interface

[2] **ISO/IEC 14443-3: July 2018**

Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anti-collision

[3] **AN10833 MIFARE Interface Platform Type Identification Procedure**

Application note, https://www.nxp.com/docs/en/application-note/AN10833.pdf

[4] **AN10834 MIFARE ISO/IEC 14443 PICC Selection**

Application note, https://www.nxp.com/docs/en/application-note/AN10834.pdf

[5] **AN13452 MIFARE Ultralight AES - features and hints**

Application note, https://www.nxp.com/docs/en/application-note/AN13452.pdf

[6] **AN1303 MIFARE Ultralight as Type 2 Tag**

Application note, https://www.nxp.com/docs/en/application-note/AN1303.pdf

[7] **AN13453 MIFARE Ultralight AES - coil design guide**

Application note, https://www.nxp.com/docs/en/application-note/AN13453.pdf

[8] **AN13454 MIFARE Ultralight AES - quick start guide**

Application note, https://www.nxp.com/docs/en/application-note/AN13454.pdf

[9] **FIPS PUB 197. Advanced Encryption Standard (AES)**

November 2001.

[10] **ISO/IEC 10116: Information technology - Security techniques - Modes of operation for an n-bit block cipher**

International Organization for Standardization, 2017,

[12] **Contactless smart card module specification MOA8**

Delivery Type Description, BU-ID Document number 1636**

[13] **General specification for 8" wafer on UV-tape**

Delivery Type Description, BU-ID Document number 1005**

[14] **NIST Special Publication 800-38A**

National Institute of Standards and Technology (NIST).

Recommendation for BlockCipher Modes of Operation.

[15] **NIST Special Publication 800-38B**

National Institute of Standards and Technology (NIST).

Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication.

https://csrc.nist.gov/publications/detail/sp/800-38b/final

[16] **NIST Special Publication 800-90B**

Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018.

[17] **NIST Special Publication 800-108**

National Institute of Standards and Technology (NIST).

Recommendation for key derivation using pseudorandom functions.

[18] **Certicom Research. Sec 1**

Elliptic curve cryptography. Version 2.0, May 2009.

[19] **Certicom Research. Sec 2**

Recommended Elliptic Curve Domain Parameters. Version 2.0, January 2010.

[20] **NFC Forum Tag 2 Type Operation, Technical Specification**

NFC Forum, 31.05.2011, Version 1.0

[21] **NFC Data Exchange Format (NDEF), Technical Specification**

NFC Forum, 24.07.2006, Version 1.0

18 Revision history

Table 66. Revision history

Document ID	Release date	Data sheet status	Supersedes
MF0AES(H)x0 v.3.2	20230328	Product data sheet	MF0AES(H)x0 v.3.1
Modifications:	• Bump size changed from 60 µm to 80 µm in Section 13 and Figure 24		
MF0AES(H)x0 v.3.1	20220429	Product data sheet	MF0AES(H)x0 v.3.0
Modifications:	• Editorial changes • Section 17 "References": updated		
MF0AES(H)x0 v.3.0	20220222	Product data sheet	MF0AES(H)x0 v.2.0
Modifications:	• Data sheet status changed into "Product data sheet"		
MF0AES(H)x0 v.2.0	20220204	Preliminary data sheet	MF0AES(H)x0 v.1.2
Modifications:	• CMAC inclusion in the commands		
MF0AES(H)x0 v.1.2	20220117	Objective data sheet	MF0AES(H)x0 v.1.1
Modifications:	• PROT bit in Configuration parameter description updated		
MF0AES(H)x0 v.1.1	20211220	Objective data sheet	MF0AES(H)x0 v.1.0
Modifications:	• General description • Table15 • Wafer specification		
MF0AES(H)x0 v.1.0	20211006	Objective data sheet	MF0AES(H)x0 v.0.3
Modifications:	• General update		
MF0AES(H)x0 v.0.3	20210716	Objective data sheet	MF0AES(H)x0 v.0.2
Modifications:	• General update		
MF0AES(H)x0 v.0.2	20200423	Objective data sheet	MF0AES(H)x0 v.0.1
Modifications:	• General update		
MF0AES(H)x0 v.0.1	20200221	Objective data sheet	-

19 Legal information

19.1 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.

19.2 Definitions

Draft — A draft status on a document indicates that 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 in a draft version of a document 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.

Product specification — The information and data provided in a Product data sheet shall define the specification of the product as agreed between NXP Semiconductors and its customer, unless NXP Semiconductors and customer have explicitly agreed otherwise in writing. In no event however, shall an agreement be valid in which the NXP Semiconductors product is deemed to offer functions and qualities beyond those described in the Product data sheet.

19.3 Disclaimers

Limited warranty and liability — 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. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

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 life support, life-critical or safety-critical systems or 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 and its suppliers accept 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.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

Terms and conditions of commercial 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, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

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.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Suitability for use in non-automotive qualified products — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

NXP B.V. - NXP B.V. is not an operating company and it does not distribute or sell products.

19.4 Licenses

Purchase of NXP ICs with NFC technology — Purchase of an NXP Semiconductors IC that complies with one of the Near Field Communication (NFC) standards ISO/IEC 18092 and ISO/IEC 21481 does not convey an implied license under any patent right infringed by implementation of any of those standards. Purchase of NXP Semiconductors IC does not include a license to any NXP patent (or other IP right) covering combinations of those products with other products, whether hardware or software.

19.5 Trademarks

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

NXP — wordmark and logo are trademarks of NXP B.V.

DESFire — is a trademark of NXP B.V.

MIFARE — is a trademark of NXP B.V.

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

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

Tables

Figures

Contents

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

Date of release: 28 March 2023
Document identifier: MF0AES_H_20