MF1PLUSx0y1

Mainstream contactless smart card IC for fast and easy solution development

Rev. 3.2 — 21 February 2011
163532

Product short data sheet
PUBLIC

1. General description

Migrate classic contactless smart card systems to the next security level! MIFARE Plus brings benchmark security to mainstream contactless smart card applications. It is the only mainstream IC compatible with MIFARE Classic 1K (MF1ICS50) and MIFARE Classic 4K (MF1ICS70) which offers an upgrade path for existing infrastructure and services.

After the security upgrade, MIFARE Plus uses AES-128 (Advanced Encryption Standard) for authentication, data integrity and encryption. MIFARE Plus is based on open global standards for both air interface and cryptographic methods at the highest security level.

MIFARE Plus is available in two versions: MIFARE Plus X and MIFARE Plus S.

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

2. Features and benefits

- 2 kB or 4 kB EEPROM
- Simple fixed memory structure compatible with MIFARE Classic 1K and MIFARE Classic 4K
- Memory structure identical to MIFARE Classic 4K (sectors, blocks)
- Access conditions freely configurable
- Supports ISO/IEC 14443-3[1] UIDs (4-byte UID, 4 Byte NUID, 7-byte UID), optional support of random IDs
- Multi-sector authentication, Multi-block read and write
- AES-128 used for authenticity, confidentiality and integrity
- Anti-tearing mechanism for writing AES keys
- Keys can be stored as MIFARE CRYPTO1 keys (2 × 48-bit per sector) and as AES keys (2 × 128-bit per sector)
- Full support of virtual card concept
- Proximity check
- Communication speed up to 848 kbit/s

1. ISO/IEC 14443-x used in this data sheet refers to ISO/IEC 14443 Type A.

- Number of single write operations: 200000 cycles (typical)
- Common Criteria Certification: EAL4+

3. Applications

- Public transportation
- Access management such as employee, school or campus cards
- Electronic toll collection
- Closed loop micro payment
- Car parking
- Internet cafés
- Loyalty programs

4. Quick reference data

Table 1. Quick reference data

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
C_i	input capacitance	T_{amb} = 22 °C; f_i = 13.56 MHz; 2.8 V RMS	[1]	15.0	17.0	19.04	pF
f_i	input frequency			-	13.56	-	MHz
EEPROM characteristics							
t_{ret}	retention time	T_{amb} = 22 °C		10	-	-	year
$N_{endu(W)}$	write endurance	T_{amb} = 22 °C; excluding anti-tearing for AES keys or sector trailers in security level 3		100000	200000	-	cycle

[1] Measured with LCR meter.

5. Ordering information

Table 2. Ordering information

Type number	Package			
	Commercial name	Name	Description	Version
MF1PLUS8001DUD/03	FFC	-	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECS-II format) see Ref. 3, 4 kB EEPROM, 7-byte UID, L1 card	-
MF1PLUS8011DUD/03	FFC	-	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECS-II format) see Ref. 3, 4 kB EEPROM, 4-byte UID, L1 card	-
MF1PLUS8031DUD/03	FFC	-	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECS-II format) see Ref. 3, 4 kB EEPROM, 4-byte NUID, L1 card	-
MF1PLUS8001DA4/03	MOA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape, 4 kB EEPROM, 7-byte UID, L1 card	SOT500-2
MF1PLUS8011DA4/03	MOA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape, 4 kB EEPROM, 4-byte UID, L1 card	SOT500-2
MF1PLUS8031DA4/03	MOA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape, 4 kB EEPROM, 4-byte NUID, L1 card	SOT500-2
MF1PLUS6001DUD/03	FFC	-	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECS-II format) see Ref. 3, 2 kB EEPROM, 7-byte UID, L1 card	-
MF1PLUS6011DUD/03	FFC	-	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECS-II format) see Ref. 3, 2 kB EEPROM, 4-byte UID, L1 card	-
MF1PLUS6031DUD/03	FFC	-	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECS-II format) see Ref. 3, 2 kB EEPROM, 4-byte NUID, L1 card	-
MF1PLUS6001DA4/03	MOA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape, 2 kB EEPROM, 7-byte UID, L1 card	SOT500-2
MF1PLUS6011DA4/03	MOA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape, 2 kB EEPROM, 4-byte UID, L1 card	SOT500-2
MF1PLUS6031DA4/03	MOA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape, 2 kB EEPROM, 4-byte NUID, L1 card	SOT500-2
MF1PLUS8001DUD/13	FFC	-	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECS-II format) see Ref. 3, 4 kB EEPROM, 7-byte UID, no security level 1 or 2, L3 card	-

Table 2. Ordering information *…continued*

Type number	Package			
	Commercial name	Name	Description	Version
MF1PLUS8001DA4/13	MOA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape, 4 kB EEPROM, 7-byte UID, no security level 1 or 2, L3 card	SOT500-2
MF1PLUS6001DUD/13	FFC	-	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECS-II format) see Ref. 3, 2 kB EEPROM, 7-byte UID, no security level 1 or 2, L3 card	-
MF1PLUS6001DA4/13	MOA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape, 2 kB EEPROM, 7-byte UID, no security level 1or 2, L3 card	SOT500-2

6. Block diagram

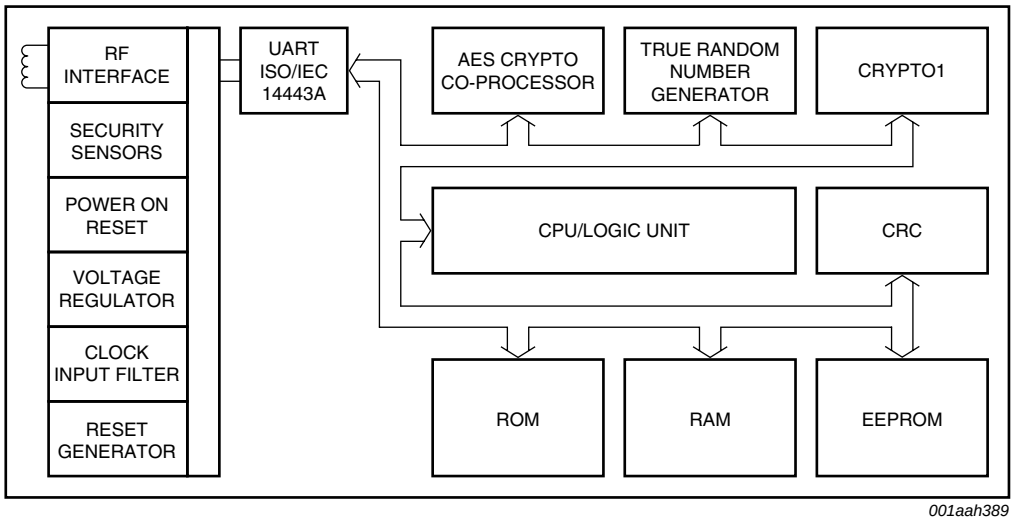

Fig 1. Block diagram

7. Pinning information

7.1 Smart card contactless module

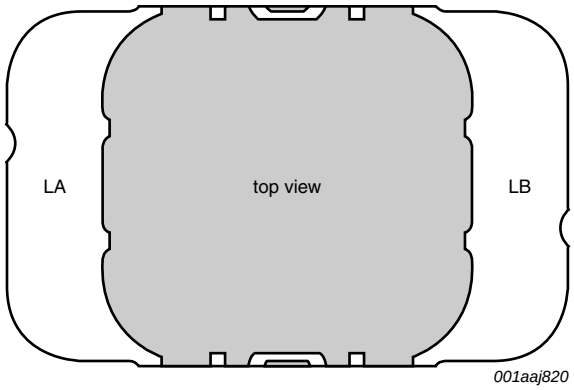

Fig 2. Contact assignments for SOT500-2 (MOA4)

Table 3. Bonding pad assignments to smart card contactless module

Contactless interface module		MF1PLUSx0y1DA4/03 and /13
Antenna contacts	**Symbol**	**Description**
LA	LA	antenna coil connection LA
LB	LB	antenna coil connection LB

8. Functional description

8.1 Memory organization

The 4 kB EEPROM memory (MF1PLUS80x) is organized in 32 sectors of 4 blocks and in 8 sectors of 16 blocks. The 2 kB EEPROM memory (MF1PLUS60x) is organized in 32 sectors of 4 blocks.

One block consists of 16 bytes.

SECTOR	BLOCK	BYTE NUMBERS WITHIN A BLOCK															DESCRIPTION
		0	1	2	3	4	5(1)	6	7	8	9	10	11	12	13	14	15	
39	15	CRYPTO1 key A						access bytes				CRYPTO1 key B or data						sector trailer 39
	14																	data
	13																	data
	...																	...
	...																	...
	2																	data
	1																	data
	0																	data
	...																	...
	...																	...
	...																	...
32	15	CRYPTO1 key A						access bytes				CRYPTO1 key B or data						sector trailer 32
	14																	data
	13																	data
	...																	...
	...																	...
	2																	data
	1																	data
	0																	data
31	3	CRYPTO1 key A						access bytes				CRYPTO1 key B or data						sector trailer 31
	2																	data
	1																	data
	0																	data
	...																	...
	...																	...
	...																	...
0	3	CRYPTO1 key A						access bytes				CRYPTO1 key B or data						sector trailer 0
	2																	data
	1																	data
	0																	manufacturer data

001aaj843

(1) CRYPTO1 key A in security level 0, 1, 2; plain text access byte in security level 3

Fig 3. Memory organization

8.1.1 Manufacturer block

The first data block (block 0) of the first sector (sector 0) contains the PICC manufacturer data. This block is programmed and write protected during the production test.

8.1.2 Data blocks

Sectors 0_D to 31_D contain 3 blocks each and sectors 32_D to 39_D contain 15 blocks for data storage. The data blocks can be configured using the access bits as:

- read/write blocks for storing binary data
- value blocks (only available in security level 1)

Value blocks are special counters where the stored value can be manipulated with specific commands such as MF Increment, MF Decrement and MF Transfer.

These value blocks have a fixed data format enabling error detection and correction with backup management to be performed.

The MIFARE Plus X provides two further commands which can be used to optimize performance when using value blocks. These are:

- MF Increment Decrement
- MF Decrement Transfer

A successful mutual authentication is required to allow any data operation.

8.1.2.1 Access conditions

The access conditions for every data block and the sector trailer itself are stored in the sector trailer of the corresponding sector.

The access bits control the rights of memory operations using the secret keys A and B. The access conditions may be altered after authentication with the relevant key and the current access condition allows this operation.

Furthermore, value blocks are configured using the access bits.

8.1.3 AES keys

AES keys are not shown in the memory map. The keys are stored on top of the other data and can be updated and used by referencing the Key Number. In security level 3, anti-tearing is supported for the update of AES keys as well as for the update of the sector trailer. In security level 2, anti-tearing is supported only for the update of AES keys. This anti-tearing mechanism is done by the PICC itself. The EEPROM stays in a defined status, even if the PICC is removed from the electromagnetic field during the write operation.

8.1.4 Proximity check

The security level 3 offers a feature to verify that the PICC is in close proximity to the PCD. This functionality can be used to effectively prevent relay attacks.

The proximity check is based on a precise time measurement of challenge-response pairs in combination with cryptographic methods.

8.1.5 Multi-sector authentication

A new feature has been provided in security level 2 and 3 for data which is spread over multiple sectors to improve transaction performance.

Providing that such sectors are secured with identical keys (key value and key type) only one authentication is required to read and/or write data from these sectors. There is no need to re-authenticate when accessing any data within these sectors. Therefore it is possible to configure a card in such a way that operating with only one authentication is needed in security level 3 to access all sectors. The same applies also for security level 2 authentications (one is AES-based the other one is CRYPTO1-based)

8.1.6 Originality function

The originality function is implemented by an AES authentication with the originality key. The authentication is performed in ISO/IEC 14443-4 protocol layer.

8.2 Card activation and communication protocol

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

There are three different versions of the PICC. The UID is programmed into a locked part of the NV-memory reserved for the manufacturer:

- unique 7-byte serial number
- unique 4-byte serial number
- non-unique 4-byte serial number

Due to security and system requirements, these bytes are write-protected after being programmed by the PICC manufacturer at production.

Remark: The programmed 4-byte NUID serial number is not globally unique which has to be considered in the contactless system design. See Ref. 11 for further information regarding handling of UIDs.

The customer must decide which UID length to use when ordering the product, see Table 2 for ordering information.

During personalization, the PICC can be configured to support Random ID in security level 3. The user can configure whether Random ID or fixed UID shall be used. According to ISO/IEC 14443-3 the first anticollision loop (see Ref. 5) returns the Random Number Tag 08h, the 3-byte Random Number and the BCC, if Random ID is used. The retrieval of the UID in this case can be done using the Virtual Card Support Last command, see Ref. 3 or by reading out block 0.

8.2.1 Backwards compatibility protocol

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

- Frame definition: according to ISO/IEC 14443-3
- Bit encoding: according to ISO/IEC 14443-2
- Error code handling: handling is proprietary as error codes are formatted in half bytes.
- Command specification: commands are proprietary. Please use the specification as in Ref. 1 and Ref. 2 and the additional commands which are only implemented in MIFARE Plus as described in this document and in Ref. 3.

The following security levels can run on this protocol:

- Security Level 0
- Security Level 1

- Security Level 2

8.2.2 ISO/IEC 14443-4 Protocol

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

- Security Level 0: all commands
- Security Level 1: only the security level switch and originality function
- Security Level 2: updating AES keys and configuration blocks as well as the security level switch and originality function
- Security Level 3: all commands

8.3 Security level switching

The MIFARE Plus X offers a unique feature to support migration from CRYPTO1 based systems to AES based operation. The migration on the card-side is done using different security levels supporting different cryptographic algorithms and protocols. There are four security levels:

- Security level 0: initial delivery configuration, used for card personalization
- Security level 1: backwards functional compatibility mode (with MIFARE Classic 1K and MIFARE Classic 4K) with optional AES authentication
- Security level 2: 3-Pass authentication based on AES followed by MIFARE CRYPTO1 authentication, communication secured by MIFARE CRYPTO1

  The MIFARE CRYPTO1 uses session keys derived from the AES and MIFARE CRYPTO1 authentication.
- Security level 3: 3-Pass authentication based on AES, data manipulation commands secured by AES encryption and an AES based MACing method

If the card is a L3 card the Commit Perso command will switch the card directly from security level 0 to security level 3 instead of security level 1.

The security level switching (i.e. from security level 1 to security level 3) is performed using the dedicated AES authentication switching keys.

The security level can only be switched from a lower to a higher level, never in the opposite direction.

8.4 Security level 0

Security level 0 is the initial delivery configuration of the PICC. The card can be operated either using the backwards compatibility protocol or the ISO/IEC 14443-4 protocol.

In this level, the card can be personalized including the programming of user data as well as CRYPTO1 and/or AES keys. In addition, the originality function can be used.

The following mandatory AES keys must be written, using the Write Perso command before the PICC can be switched to security level 1 or security level 3 (for L3 card).

Security level switching is performed using the Commit Perso command:

- Card Configuration Key
- Card Master Key
- Level 2 Switch Key (for L1 card)
- Level 3 Switch Key (for L1 card)

Using the originality function, it is possible to verify that the chip is a genuine NXP Semiconductors MIFARE Plus.

8.5 Security level 1

Security level 1 offers the same functionality as a MIFARE Classic 1K and MIFARE Classic 4K using the backwards compatibility protocol. The MIFARE Classic 1K and MIFARE Classic 4K products are specified in Ref. 1 and Ref. 2.

Furthermore, an optional AES authentication is available in this level without affecting the MIFARE Classic 1K and MIFARE Classic 4K functionality. The authenticity of the card can be proven using strong cryptographic means with this additional functionality.

The timings may differ from the MIFARE Classic 1K and MIFARE Classic 4K products.

Using the originality function, it is possible to verify that the chip is a genuine NXP Semiconductors MIFARE Plus.

8.6 Security level 2

Security level 2 also offers the functionality of a MIFARE Classic 1K and MIFARE Classic 4K using the backwards compatibility protocol. The significant difference compared to security level 1 is that an AES authentication is mandatory and that the CRYPTO1 keys are derived for each session using the results from the AES authentication, rather than being constant for a specific sector.

The timings may differ from the MIFARE Classic 1K and MIFARE Classic 4K products.

In security level 2, the following keys are assigned to each sector:

- Two AES keys (key A and key B) these keys are also used in security level 3

  two CRYPTO1 keys (key A and key B) these keys are also used in security level 1

The access conditions are set in the sector trailer as in MIFARE Classic 1K and MIFARE Classic 4K.

Using the originality function, it is possible to verify that the chip is a genuine NXP Semiconductors MIFARE Plus.

8.7 Security level 3

The operation in security level 3 is solely based on the ISO/IEC 14443-4 protocol layer. The usage of the backwards compatibility protocol is not possible.

In security level 3, a mandatory AES authentication between PICC and reader is conducted, where two keys are generated as a function of the random numbers from the PICC and the reader as well as of the shared key.

These two session keys are used to secure the data which is exchanged on the interface between the card and reader. One of the two keys is used to ensure the confidentiality of the command and the response while the other key ensures the integrity of the command and the response.

The reader can decide which security needs to be used in the communication between PICC and reader. In the simplest case, all commands are secured by a MAC, such that the PICC will only accept commands from the authenticated reader. Any message tampering is detected by verifying the MAC. All responses are appended by a MAC to prove to the reader that neither the command nor the response have been compromised.

If performance is the highest priority, the card can be configured to omit the MAC for read commands. The card then accepts read commands without knowing whether they are authentic. However, there is a mechanism to prove to the reader that the read response is resulting from the unmodified read command that it sent.

Other commands, like write commands, always need to have a MAC appended to ensure that no memory changes are carried out without proving the authenticity of the command.

The reader can decide for each command whether a MAC is included in the response. When the appropriate MAC is received, due to linked MACs the reader knows that the command and commands before it were properly executed.

All commands between two consecutive First Authenticate commands belong to one transaction and the MACing mechanism assures integrity of the whole transaction.

If the MAC on read responses is omitted, the integrity of all read responses within one session can still be verified by including a MAC on one read response before issuing the next First or Following Authenticate command.

If performance matters more than confidentiality of the transaction, each data block in a sector can be configured to allow or disallow sending/receiving plain data.

9. Look-up tables

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

Table 4. ISO/IEC 14443-3

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

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

Table 5. ISO/IEC 14443-4

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

Please find more information on ISO/IEC 14443-3 in Ref. 5 as well as on the settings of ATQA, SAK and ATS in Ref. 4.

9.3 Security level 0 command overview

Table 6. Security level 0 command overview

Command	Description
Write Perso	pre-personalization of AES keys and all blocks
Commit Perso	switch to security level 1 (L1 card) or security level 3 (L3 card)
First Authenticate (part 1)	first authenticate
Following Authenticate (part 1)	following authenticate
Authenticate (part 2)	second authentication step

9.4 Security level 1 command overview

Table 7. Security level 1 command overview

MF1ICS50xx, MF1ICS70xx, MF1ICS20xx commands	Description
MF Authenticate key A	authentication with key A
MF Authenticate key B	authentication with key B
MF Read	reading data
MF Write	writing data
MF Increment	incrementing a value
MF Decrement	decrementing a value
MF Restore	restoring a value
MF Transfer	transferring a value
Commands using backwards compatibility protocol; see Section 8.2.1	
Following Authenticate (part 1)	following authenticate; protocol used as described in Section 8.2.1
Authenticate (part 2)	second authentication step; protocol used as described in Section 8.2.1
Command set for security level switch and originality function using ISO 14443-4 protocol	
First Authenticate (part 1)	first authenticate
Following Authenticate (part 1)	following authenticate
Authenticate (part 2)	second authentication step

9.5 Security level 2 command overview

Table 8. Security level 2 command overview

Command	Description
Commands using backwards compatibility protocol; see Section 8.2.1	
Following Authenticate (part 1)	following authenticate
Authenticate (part 2)	second authentication step
MF1ICS50xx, MF1ICS70xx commands	
MF Authenticate Key A	authentication with key A
MF Authenticate Key B	authentication with key B
MF Read	reading data
MF Write	writing data
MF Decrement	decrementing a value
MF Increment	incrementing a value
MF Restore	restoring a value
MF Transfer	transferring a value
Multi Block Read	reading multiple blocks (up to sector length)
Multi Block Write	writing multiple blocks (up to sector length)
Command set for updating AES keys and configuration blocks as well as security level switch and originality function using ISO 14443-4	
First Authenticate (part 1)	first authenticate
Following Authenticate (part 1)	following authenticate
Authenticate (part 2)	second authentication step
Write	writing encrypted, no MAC on response, MAC on command
Write MACed	writing encrypted, MAC on response, MAC on command

9.6 Security level 3 command overview

Table 9. Security level 3 command overview

Command	Description
MIFARE Plus commands	
First Authenticate (part 1)	first authenticate
Following Authenticate (part 1)	following authenticate
Authenticate (part 2)	second authentication step
ResetAuth	reset the authentication step
READ commands	
Read	reading encrypted, no MAC on response, MAC on command
Read MACed	reading encrypted, MAC on response, MAC on command
Read Plain	reading in plain, no MAC on response, MAC on command
Read Plain MACed	reading in plain, MAC on response, MAC on command
Read UnMACed	reading encrypted, no MAC on response, no MAC on command
Read UnMACed, Response MACed	reading encrypted, MAC on response, no MAC on command
Read Plain UnMACed	reading in plain, no MAC on response, no MAC on command

Table 9. Security level 3 command overview *...continued*

Command	Description
Read Plain UnMACed, Response MACed	reading in plain, MAC on response, no MAC on command
Write commands	
Write	writing encrypted, no MAC on response, MAC on command
Write MACed	writing encrypted, MAC on response, MAC on command
Write Plain	writing in plain, no MAC on response, MAC on command
Write Plain MACed	writing in plain, MAC on response, MAC on command
VALUE operations	
Increment	incrementing a value encrypted, no MAC on response, MAC on command
Increment MACed	incrementing a value encrypted, MAC on response, MAC on command
Decrement	decrementing a value encrypted, no MAC on response, MAC on command
Decrement MACed	decrementing a value encrypted, MAC on response, MAC on command
Transfer	transferring a value, no MAC on response, MAC on command
Transfer MACed	transferring a value, MAC on response, MAC on command
Increment Transfer	combined incrementing and transferring a value encrypted, no MAC on response, MAC on command
Increment Transfer MACed	combined incrementing and transferring a value encrypted, MAC on response, MAC on command
Decrement Transfer	combined decrementing and transferring a value encrypted, no MAC on response, MAC on command
Decrement Transfer MACed	combined decrementing and transferring a value encrypted, MAC on response, MAC on command
Restore	restoring a value, no MAC on response, MAC on command
Restore MACed	restoring a value, MAC on response, MAC on command
Proximity check and virtual card concept	
Prepare Proximity Check	prepare for the proximity check
Proximity Check	perform the precise measurement for the proximity check
Verify Proximity Check	verify the proximity check
Virtual Card Support	check, if the virtual card concept is supported
Virtual Card Support Last	check if the virtual card concept is supported, communicate PCD capabilities and retrieve the UID
Select Virtual Card	select the virtual card
Deselect Virtual Card	deselect the virtual card

10. Limiting values

Table 10. Limiting values

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

Symbol	Parameter	Conditions	Min	Max[1][2]	Unit
I_I	input current		-	30	mA
P_{tot}/pack	total power dissipation per package		-	200	mW
T_{stg}	storage temperature		–55	125	°C
T_{amb}	ambient temperature		–25	70	°C
V_{ESD}	electrostatic discharge voltage	[3]	2	-	kV
I_{lu}	latch-up current		±100	-	mA

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

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

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

11. Abbreviations

Table 11. Abbreviations

Acronym	Description
AES	Advanced Encryption Standard
ATQA	Answer To reQuest
ATS	Answer To Select
BCC	Bit Count Check
EEPROM	Electrically Erasable Programmable Read-Only Memory
LCR	L = inductance, Capacitance, Resistance (LCR meter)
MAC	Message Authentication Code
NUID	Non-Unique IDentifier
NV	Non-Volatile memory
PCD	Proximity Coupling Device (Contactless Reader)
PICC	Proximity Integrated Circuit Card (Contactless Card)
PPS	Protocol Parameter Selection
RATS	Request Answer To Select
REQA	REQuest Answer
SAK	Select AcKnowledge, type A
SECS-II	SEMI Equipment Communications Standard part 2
SEMI	Semiconductors Equipment and Materials International
UID	Unique IDentifier
VC	Virtual Card, one MIFARE Plus PICC is one virtual card
WUPA	Wake Up Protocol A

12. References

[1] **Data sheet — MF1ICS50 Functional specification, BU-ID Doc. No. 0010**[2].

[2] **Data sheet — MF1ICS70 Functional specification, BU-ID Doc. No. 0435**.

[3] **Data sheet — M1PLUSx0y1 MIFARE Plus functional specification, BU-ID Doc. No. 1637**.

[4] **Application note — MIFARE Type identification procedure, BU-ID Doc. No. 1843**.

[5] **Application note — ISO/IEC 14443 PICC selection, BU-ID Doc. No. 1308**.

[6] **NIST Special Publication 800-38A — Recommendation for block cipher modes of operation: methods and techniques, 2001.

[7] **NIST Special Publication 800-38B — Recommendation for block cipher modes of operation: The CMAC mode for authentication.

[8] **ISO/IEC Standard — ISO/IEC 14443 Identification cards - contactless integrated circuit cards - proximity cards.

[9] **Recommendation for block cipher modes of operation: methods and techniques — FIPS PUB 197 ADVANCED ENCRYPTION STANDARD.

[10] **ISO/IEC Standard — ISO/IEC 9797-1 Information technology - security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher.

[11] **MIFARE and handling of UIDs — Application note, BU-ID Document number 1907**[2]

13. Revision history

Table 12. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
MF1PLUSX0Y1_SDS v.3.2	20110221	Product short data sheet	-	MF1PLUSX0Y1_SDS_31
Modifications:	• Added description and ordering information for NUID Types in Section 2, Section 5 and Section 8.2			
MF1PLUSX0Y1_SDS_31	20100419	Product short data sheet	-	163530
Modifications:	• Minor text and standardization modifications			
163530	20100211	Product short data sheet	-	163512
Modifications:	• Several editorial changes and content rephrasing • Table 1 “Quick reference data: min. value of C_i modified • Table 2 “Ordering information”: updated • Section 14 “Legal information”: updated			
163512	20090325	Objective short data sheet	-	163511
Modifications:	• New name for the product MIFARE Plus X • General update			
163511	20081113	Objective short data sheet	-	163510
163510	20080919	Objective short data sheet	-	-

2. ** ... document version number

14. Legal information

14.1 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.

14.2 Definitions

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

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

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.

14.3 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.

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 accepts no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

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

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.

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 national authorities.

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.

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.

14.4 Licenses

ICs with DPA Countermeasures functionality
LICENSED DPA™ COUNTERMEASURES — NXP ICs containing functionality implementing countermeasures to Differential Power Analysis and Simple Power Analysis are produced and sold under applicable license from Cryptography Research, Inc.

14.5 Trademarks

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

MIFARE — is a trademark of NXP B.V.

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

15. Contact information

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

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

16. Tables

17. Figures

18. Contents

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

Date of release: 21 February 2011
163532