MF1P(H)x2

MIFARE Plus EV2

Rev. 3.1 — 9 August 2021

Product short data sheet
COMPANY PUBLIC

1 General description

MIFARE Plus EV2 (MF1P(H)x2) is the latest addition to the MIFARE Plus product family with enhanced performance at best in class security and flexibility. MIFARE Plus EV2 is Common Criteria EAL5+ security certified product serving the same security certification level as demanded for banking and electronic passport contactless IC products. It is the new benchmark to the mainstream contactless smart card applications with the possibility to upgrade existing infrastructure and services in a seamless way and with minimum effort. Based on these parameters MIFARE Plus EV2 is a trusted platform targeting the secure authentication of people with an intuitive convenient user experience.

MIFARE Plus EV2 is fully backward compatible to its predecessor as well as to the MIFARE Classic EV1 products. After the card personalization MIFARE Plus EV2 allows AES (Advanced Encryption Standard) for authentication, data integrity and encryption. MIFARE Plus is based on open global standards for both air interface and cryptographic methods at the highest security level.

MIFARE Plus EV2 contains features like the fully encrypted communication mode enabling contactless applications to address privacy sensitive applications. With its optional support of Random ID, it enables compliance with latest user data protection regulations.

MIFARE Plus EV2 is fully compliant with the contactless proximity smart card protocol according to ISO/IEC 14443-4. ISO/IEC 7816-4 is supported in security level 3 based on AES protocol to making it compatible with the majority of existing contactless infrastructure devices and with NFC devices, such as NFC enabled mobile handsets. Its contactless performance supports superior user convenience and reading distances up to 10 cm.

The non-volatile memory of the MIFARE Plus EV2 is organized in sectors of blocks with either 2k or 4k byte memory to allow a seamless migration from legacy to more advanced products by a step-by-step upgrade of existing infrastructures to higher security, where needed. That is served with the possibility of sector-wise security upgrades of the card.

MIFARE Plus EV2 allows in the MIFARE Classic EV1 backward compatible mode to restrict data and value blocks as well SectorTrailers without the need to permanently lock these blocks and related SectorTrailer(s). That is enabled by restriction of an update operation to blocks configured as restricted configuration block independent of the access condition configuration of the SectorTrailer.

MIFARE Plus EV2 offers a Transaction Timer feature to allow the card issuer to configure a maximum time a transaction can take. Furthermore, a Transaction Message Authentication (TMAC) is supported that allows operators of, e.g., payment applications to calculate a cryptographic checksum over the complete transaction enabling the verification of a transaction by a clearing entity.

MIFARE Plus EV2 is designed to support standards Class 1 smart cards antenna designs with a 17 pF input capacitance as well as smaller form factors, i.e. key fobs,

wristbands, by providing 70 pF input capacitance delivery forms. This ensures high user convenience throughout different form factors. This ensures high user convenience throughout different form factors.

Furthermore, MIFARE Plus EV2 offers two ways to check the originality of the product. Either based on a symmetric AES authentication with the 128-bit AES originality key or an asymmetric ECC-based NXP Originality Signature to verify the origin of a ticket with a certain confidence.

2 Features and benefits

- 2 kB, 4 kB non-volatile memory
- 7-byte UID, 4-byte NUID
- Supports ISO/IEC 14443-3 [1] Random ID for all UID types
- Communication speed up to 848 kbit/s
- Freely configurable access conditions
- Security Level (SL) concept for seamless migration from legacy infrastructure to high-level SL3 security
- Sequential writing of the personalization keys (in SL0)
- AES-128 cryptography for authentication and secure messaging (optional in SL1, mandatory in SL3)
- SL3 CardSecurityLevel or sector-by-sector security level upgrade possible (SectorSecurityLevel)
- SL1SL3Mix mode to allow secure backend connections into SL1 sectors
- Configuration block to restrict update operations for Data/Value Blocks and Sector Trailers in the MIFARE Classic EV1 backwards compatible mode
- Multi-sector authentication, multi-block read and write
- Anti-tearing mechanism for AES keys and for data block writing
- Virtual card concept using ISO/IEC 7816-4 compliant selection method
- Proximity check fully ISO/IEC 14443-3 compliant
- Transaction MAC on value and data blocks
- Transaction Timer to mitigate Man-in-the-Middle attacks
- Direct commit personalization from SL0 to SL1 or SL3
- Common Criteria Certification: EAL5+ [2]
- ECC-based NXP Originality Signature
- AES-based originality key leveraging the AES authentication

1 ISO/IEC 14443-x used in this data-sheet refers to ISO/IEC 14443 Type A.
2 (AVA_VAN.5 implying resistance against attackers with HIGH attack potential)

3 Applications

- Public transportation
- Access management
- Event ticketing
- Electronic voucher
- Loyalty card
- Micro-payment

4 Quick reference data

Table 1. Quick reference data

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
f_i	input frequency		-	13.56	-	MHz
$V_{min, LA-LB}$	LA/LB minimum voltage at H_{min}		-	2.2	-	V
Z_{LA-LB}	LA/LB impedance at H_{min}		-	1.2	-	kΩ
C_i	input capacitance MF1Px2 [1]	T_{amb} = 25 °C°C	-	17	-	pF
	input capacitance MF1PHx2 [1]	T_{amb} = 25 °C°C	-	66.5	-	pF
Non-Volatile memory characteristics characteristics						
t_{ret}	retention time	T_{amb} = 25 °C	25	-	-	year
$N_{endu(W)}$	write endurance	T_{amb} = 25 °C	200,000	1,000,000	-	cycle

[1] f_i = 13.56 MHz; 2.2 V RMS

5 Ordering information

Table 2. MF1Px2

Type number	Package			Configuration		
	Name	Description	Version	Non-Volatile	Input Cap.	UID
MF1P2201DUD/00	FFC	12-inch wafer (Sawn, 120 µm thickness) [1]	SOT500-2	2k byte	17 pF	7-byte
MF1P2231DUD/00	FFC	12-inch wafer (Sawn, 120 µm thickness) [1]	SOT500-2	2k byte	17 pF	4-byte NUID
MF1P4201DUD/00	FFC	12-inch wafer (Sawn, 120 µm thickness) [1]	SOT500-2	4k byte	17 pF	7-byte
MF1P4231DUD/00	FFC	12-inch wafer (Sawn, 120 µm thickness) [1]	SOT500-2	4k byte	17 pF	4-byte NUID
MF1P2200DA8/00	MOA8	Plastic leadless module carrier package [2]	SOT500-4	2k byte	17 pF	7-byte
MF1P2230DA8/00	MOA8	Plastic leadless module carrier package [2]	SOT500-4	2k byte	17 pF	4-byte NUID
MF1P4200DA8/00	MOA8	Plastic leadless module carrier package [2]	SOT500-4	4k byte	17 pF	7-byte
MF1P4230DA8/00	MOA8	Plastic leadless module carrier package [2]	SOT500-4	4k byte	17 pF	4-byte NUID
MF1P2200DA4/00	MOA4	Plastic leadless module carrier package [2]	SOT500-2	2k byte	17 pF	7-byte
MF1P2230DA4/00	MOA4	Plastic leadless module carrier package [2]	SOT500-2	2k byte	17 pF	4-byte NUID
MF1P4200DA4/00	MOA4	Plastic leadless module carrier package [2]	SOT500-2	4k byte	17 pF	7-byte
MF1P4230DA4/00	MOA4	Plastic leadless module carrier package [2]	SOT500-2	4k byte	17 pF	4-byte NUID

[1] 12-inch wafer (Sawn; on film frame carrier; electronic fail die marking according to SECS-II format), see [1]
[2] Plastic lead-less module carrier package; 35 mm wide tape

Table 3. MF1PHx2

Type number	Package			Configuration		
	Name	Description	Version	Non-Volatile	Input Cap.	UID
MF1PH2201DUD/00	FFC	12-inch wafer (Sawn, 120 µm thickness) [1]	SOT500-2	2k byte	70 pF	7-byte
MF1PH2231DUD/00	FFC	12-inch wafer (Sawn, 120 µm thickness) [1]	SOT500-2	2k byte	70 pF	4-byte NUID
MF1PH4201DUD/00	FFC	12-inch wafer (Sawn, 120 µm thickness) [1]	SOT500-2	4k byte	70 pF	7-byte
MF1PH4231DUD/00	FFC	12-inch wafer (Sawn, 120 µm thickness) [1]	SOT500-2	4k byte	70 pF	4-byte NUID
MF1PH2200DA8/00	MOA8	Plastic leadless module carrier package [2]	SOT500-4	2k byte	70 pF	7-byte
MF1PH2230DA8/00	MOA8	Plastic leadless module carrier package [2]	SOT500-4	2k byte	70 pF	4-byte NUID
MF1PH4200DA8/00	MOA8	Plastic leadless module carrier package [2]	SOT500-4	4k byte	70 pF	7-byte
MF1PH4230DA8/00	MOA8	Plastic leadless module carrier package [2]	SOT500-4	4k byte	70 pF	4-byte NUID
MF1PH2200DA4/00	MOA4	Plastic leadless module carrier package [2]	SOT500-2	2k byte	70 pF	7-byte
MF1PH2230DA4/00	MOA4	Plastic leadless module carrier package [2]	SOT500-2	2k byte	70 pF	4-byte NUID
MF1PH4200DA4/00	MOA4	Plastic leadless module carrier package [2]	SOT500-2	4k byte	70 pF	7-byte
MF1PH4230DA4/00	MOA4	Plastic leadless module carrier package [2]	SOT500-2	4k byte	70 pF	4-byte NUID

[1] 12-inch wafer (Sawn; on film frame carrier; electronic fail die marking according to SECS-II format), see [1]
[2] Plastic lead-less module carrier package; 35 mm wide tape

6 Block diagram

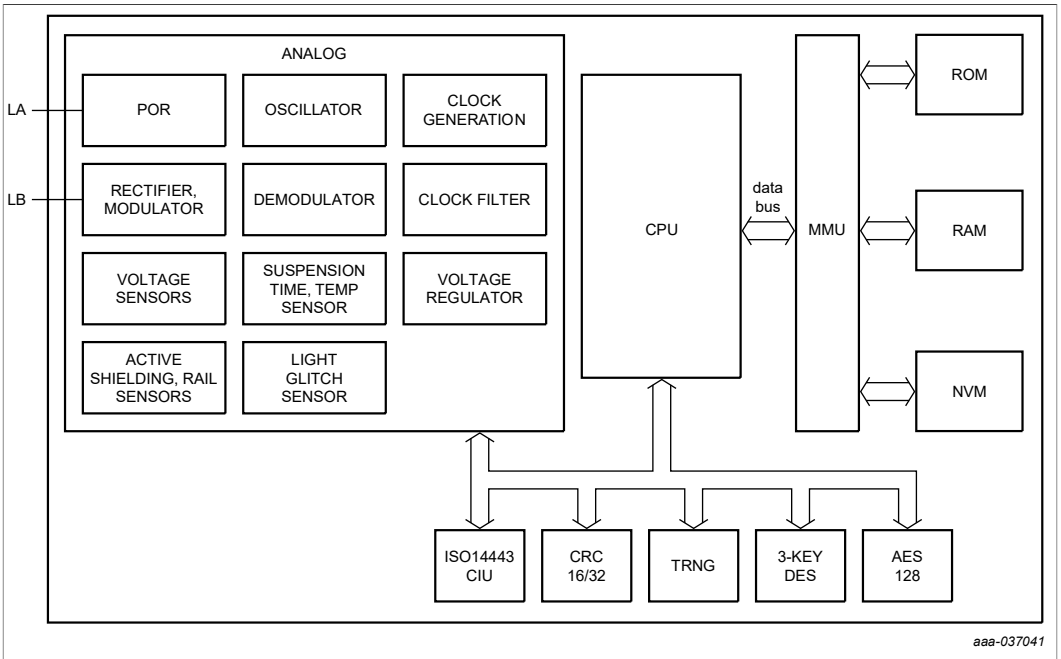


Figure 1. Block diagram

7 Pinning information

7.1 Pinning

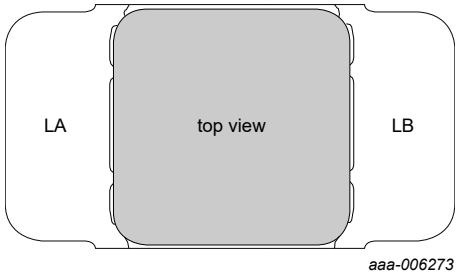


Figure 2. Pin configuration for SOT500-4 (MOA8)

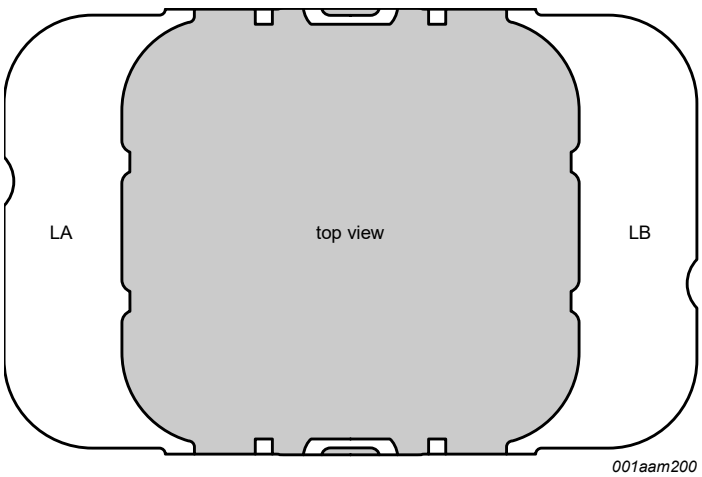


Figure 3. Pin configuration for SOT500-2 (MOA4)

7.2 Pin description

Table 4. Pin description (MOA4 and MOB6)

Symbol	Pin	Description
LA	LA	antenna coil connection LA
LB	LB	antenna coil connection LB

8 Functional description

8.1 Memory organization

The non-volatile memory of the MF1P(H)22 is organized in 32 sectors of 4 blocks (from sector 0d to 31d). The MF1P(H)42 has in addition 8 sectors of 16 blocks (from sector 32d to 39d). Each block consists of 16 bytes.

In the block 0 of sector 0 are stored the NXP manufacturer data of the IC (see Section 8.1.1) while the upper block of each sector contains the sector trailer (see Section 8.1.3). The remaining blocks of each sector can be used to store data and are called DaVaBlocks (see Section 8.1.2)

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

aaa-037343

1. CRYPTO1 KeyA in SL0 and SL1
   In SL3 the first 5 bytes are unaccessible and RFU
   Plaintext access byte in SL3 (see Figure 8)

Figure 4. Memory organization of the MF1P(H)42

Remark: The memory map does not show the AES keys and configuration blocks. The MF1P(H)22 only includes the lower 32 sectors.

8.1.1 Manufacturer block

The manufacturer data are stored in the manufacturer block, which is the first data block (block 0) of the first sector (sector 0). Due to security and system requirements, this block is write protected during production.

The manufacturer block is shown in Figure 5 and Figure 6 for the 4-byte NUID and 7-byte UID version respectively.

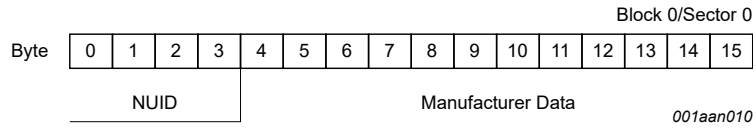


Figure 5. Manufacturer block for MF1P(H)x2 with 4-byte NUID

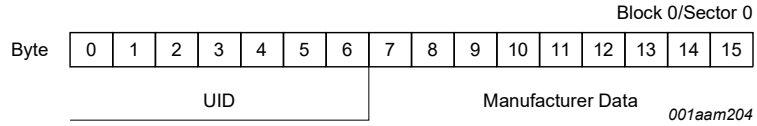


Figure 6. Manufacturer block for MF1P(H)x2 with 7-byte UID

8.1.2 Data blocks

In data blocks, it is possible to store:

- generic binary data
- value blocks to store numbers (e.g. counters)

Value blocks offer the advantage to use additional special commands to increment or decrement the numerical content (see Value operations) and require a special formatting of the block (see Section 8.1.2.1).

8.1.2.1 Value blocks

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

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

For performance reasons SL3 offers also combined increment/decrement operation with transfer operation, see Value operations.

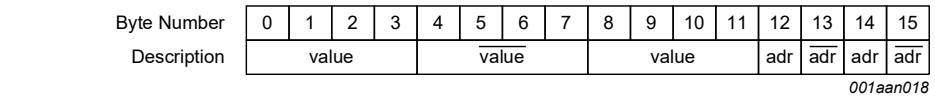


Figure 7. Value blocks formatting

An example of a valid value block format for the decimal value 1234567d and the block address 17d is shown in Table 5. First, the decimal value has to be converted to the hexadecimal representation of 0012D687h. The LSByte of the hexadecimal value is stored in Byte 0, the MSByte in Byte 3. The bit inverted hexadecimal representation of the value is FFED2978h where the LSByte is stored in Byte 4 and the MSByte in Byte 7.

The hexadecimal value of the address in the example is 11h, the bit inverted hexadecimal value is EEh.

Table 5. Value block format example

Byte Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Description	value				value				value				adr	adr	adr	adr
Values [hex]	87	D6	12	00	78	29	ED	FF	87	D6	12	00	11	EE	11	EE

The DataBlocks and ValueBlocks are together called DaVaBlocks.

8.1.3 Sector trailer

Each sector has a sector trailer in the upper block. This sector trailer is located in 4th block of each sector in the first 2 kB (sector 0 to sector 31) of the NV-memory and in 16th block of each sector in the upper 2 kB (sector 32 to sector 39) of the 4 kB NV-memory.

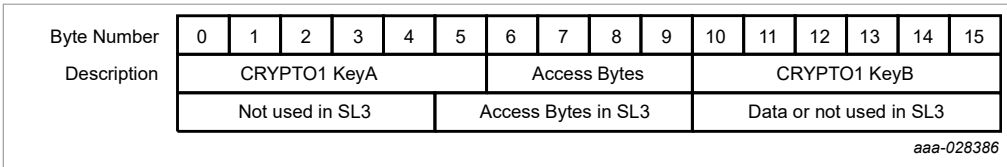


Figure 8. Sector trailer

Each sector trailer holds:

- secret CRYPTO1 keys A and B (Key B is optional)
- access conditions for the four blocks or sixteen blocks of that sector, which are stored in bytes 6 to 8. The access bits also specify the type (data or value) of the DaVaBlocks.
- byte 5 defines if plain communication can be used in SL3 after authentication. In SL3, the global DefaultPlainAC byte from the MFPConfigurationBlock is used (see MFPConfigurationBlock) unless the access condition byte for plain communication is modified for each sector separately by overwriting Byte 5 in the corresponding sector trailer. In SL1SL3Mix mode, the DefaultPlainAC byte is always used and cannot be changed by writing to the sector trailer.

In MF1P(H)x2, every write operation is secured with an anti-tearing mechanism.

8.1.3.1 Access conditions

In each sector trailer the access bytes determine the access condition (read, write, value operation) for the DaVaBlocks as well as the sector trailers itself. The access conditions

for every DaVaBlocks and sector trailer are defined by 3 bits, which are stored non-inverted and inverted in the sector trailer of the respective sector.

The access bits control the rights of memory access using the secret keys A and B. The access conditions may be altered, provided one knows the relevant key and the current access condition allows this operation.

Remark: With each memory access, the internal logic verifies the format of the access conditions. If it detects a format violation the whole sector is irreversibly blocked.

Remark: MF1P(H)x2 does not verify the format during update and will allow an inconsistent trailer data.

In the following description, the access bits are mentioned in the non-inverted mode only. The internal logic ensures that the commands are executed only after an authentication procedure.

Table 6. Access bit mapping to blocks

Access Bits	Valid Commands		Block in sectors 0 to 31	Block(s) in sectors 32 to 39 [1]	Description
$C1_3$ $C2_3$ $C3_3$	read, write	→	3	15	sector trailer
$C1_2$ $C2_2$ $C3_2$	read, write, increment, decrement, transfer, restore	→	2	10, 11, 12, 13, 14	data block
$C1_1$ $C2_1$ $C3_1$	read, write, increment, decrement, transfer, restore	→	1	5, 6, 7, 8, 9	data block
$C1_0$ $C2_0$ $C3_0$	read, write, increment, decrement, transfer, restore	→	0 [2]	0, 1, 2, 3, 4	data block

[1] Only available in MF1P(H)42
[2] Block 0 of Sector 0 is always read only

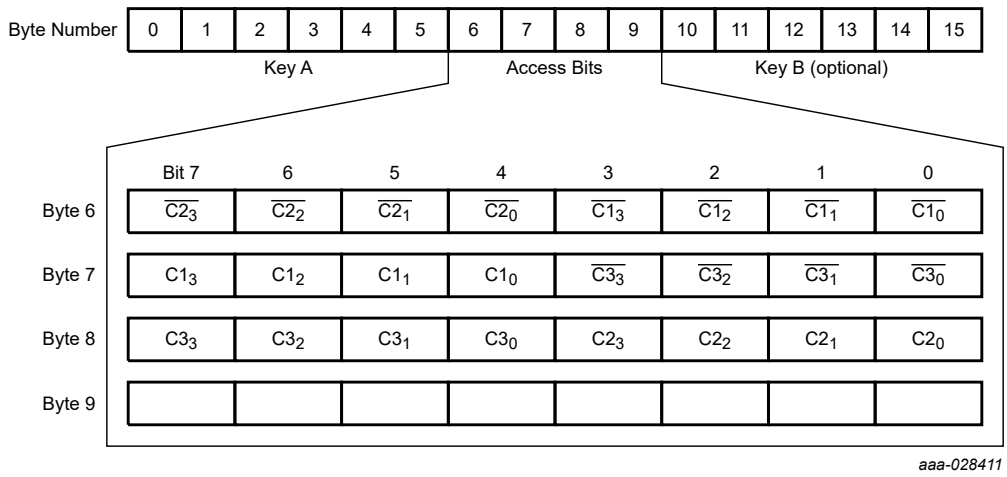


Figure 9. Access conditions for SL1

8.1.4 AES keys and other system data

Neither AES keys nor other system data like the VCSystemData blocks are 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 (see Table 1). In SL3, anti-tearing is supported for the update of AES keys as well as for the update of the sector trailer. This anti-tearing mechanism is done by the PICC itself. The non-volatile memory stays in a defined status, even if the PICC is brought out of the field during write operations. The PICC ensures that the data is either the unchanged or fully updated to the new value. It is up to the PCD to determine the state on the next PICC activation"

The write access condition described in Table 1 for the Crypto1 keys in SL1 is the same as for the AES keys in SL3.

Note: There is also a configuration block to restrict update operations (i.e. increment) for DaVaBlocks and Sector Trailers in the MIFARE Classic backwards compatibility mode in SL1, see SL1 Update Restrictions.

8.1.5 Originality function

The originality check allows verification of the genuineness of MIFARE Plus EV2. MF1P(H)x2 offers two ways to check the originality of the MIFARE Plus EV2 contactless IC: the first is based on a symmetric authentication, the second works on the verification of an asymmetric signature retrieved from the card.

The symmetric originality function is implemented by an AES authentication as described in AuthenticateFirst and AuthenticateNonFirst with the OriginalityKey1 (see Key and block number overview). The authentication with the 128-bit AES Originality key can be performed in all security levels, supporting ISO/IEC 14443-3&4 protocol layer (see also Section 8.2.2).

The asymmetric originality signature is based on ECC and only requires a public key for the verification, which is done outside the card (see [7]). The Read_Sig command can be used in both ISO/IEC 14443-3 and ISO/IEC 14443-4 protocols to retrieve the signature. If the PICC is not configured for Random ID, the command is freely available, i.e. there is no authentication required. If the PICC is configured for Random ID, an authentication with any authentication key is required.

If there is an active authentication, the secure messaging depends on the ISO/IEC 14443 activation. In SL1 after ISO/IEC 14443-3 activation, the command is encrypted with CRYPTO1 as for all other commands. In SL1 or SL3 after ISO/IEC 14443-4 activation, the command is to be MACed and the response is encrypted and MACed as shown in Figure 10. The read counter is incremented after validating the command before sending the response. This is done according to the same principles as for ReadEncryptedMAC_MACed.

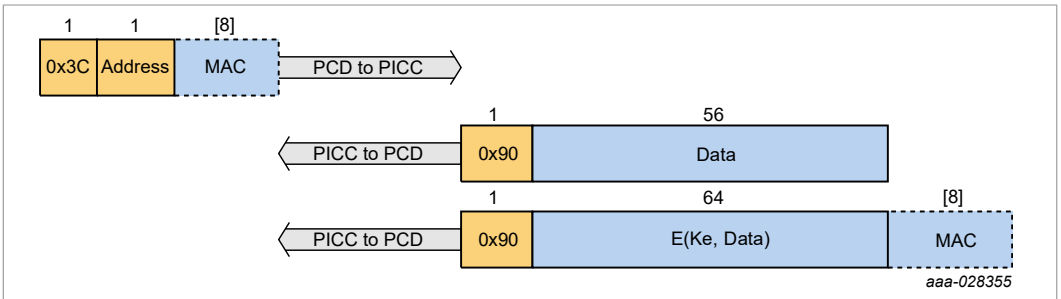


Figure 10. Read_Sig command

Table 7. Read_Sig

Name	Length	Value	Description
Description:	Retrieve the ECC originality check signature.		
Command Parameters:			
Cmd	1	3Ch	Command code.
Address	1	00h	Targeted ECC originality check signature. Other address values are RFU.
MAC	[8]	any	Optional, only present if authenticated after ISO/IEC 14443-4 activation MAC over the command
Responses:			
Resp.OK	1	90h	OK
Data	56	any	NXP Originality Signature
E(Ke, Data)	64	any	The NXPOriginalitySignature is encrypted with the session key as generated in the last authentication.
MAC	[8]	any	Optional, only present if authenticated after ISO/IEC 14443-4 activation MAC over the response
Resp.ErrCmdInvalid	1	0Bh	Not allowed without valid authentication due to Random ID configuration.
Resp.ErrFormat	1	0Ch	Command length different from 2 byte or unsupported address

8.2 Card activation and communication protocol

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

There are two different UID versions of the PICC which are programmed and locked in the manufacturer block:

1. unique 7-byte serial number (7-byte UID)
2. non-unique 4-byte serial number (4-byte NUID)

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

Remark: The programmed 4-byte NUID serial number is not globally unique which has to be considered in the contactless system design. See [19] for further information regarding handling of UIDs.

The customer has to decide which UID length to use when ordering the product (see Table 2 for ordering information).

A MF1P(H)x2 with 7-byte UID supports the additional UID configuration options as defined in [2] using the MF_PersonalizeUIDUsage command after ISO/IEC 14443-3 activation. Note that the MF_PersonalizeUIDUsage command can only be sent once.

The configuration chosen affects the ISO/IEC 14443 activation and the MIFARE Classic authentication. The defined activation sequence applies for both ISO/IEC 14443-3 and ISO/IEC 14443-4 activation, except for Sequence2 described in [2] which can only be applied with an ISO/IEC 14443-3 activation. As a consequence, if UIDF1 configuration has been chosen, the MF1P(H)x2 only supports Sequence1 for an ISO/IEC14443-4 activation.

The chosen configuration by the MF_PersonalizeUIDUsage command is reflected by the UseRID configuration byte in the FieldConfigurationBlock. On the other hand, the configuration chosen by the MF_PersonalizeUIDUsage command is overwritten by the UseRID configuration when updating the FieldConfigurationBlock, see FieldConfigurationBlock.

In case Random ID is configured, the real UID can be retrieved using the ISOSelect and ISOExternalAuthenticate commands described in ISOSelect and ISOExternalAuthenticate or by reading out block 0 of sector 0.

Remark: A full power cycle needs to be performed after each configuration change in order to ensure proper setting of the activation parameters.

8.2.1 Backwards compatibility protocol

The MIFARE Classic backwards compatibility of this product in SL1 runs on the same protocol layer as MIFARE Classic 1K/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. The used error codes (NAK - Not Acknowledge) are described in Status code overview
- Command specification: commands are proprietary. Please use the specification as in [2] and [3] and the additional commands which are only implemented in MIFARE Plus as described in this data sheet.

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. For MIFARE Plus EV2 this protocol is used in the following security levels:

- SL0: all commands
- SL1: for the sector or card level SL switch, the AES originality function, AES Key update, configuration data update, GetVersion and Read_Sig
- SL3: all commands

Remark: The ISO/IEC 14443-4 protocol is also used to operate any sector that has been switched to SL3 or SL1SL3Mix mode, when using SL3 commands.

8.2.3 ISO/IEC 7816-4 support

Next to the native command set, MIFARE Plus EV2 also supports ISO/IEC 7816-4 commands (see [9]). MF1P(H)x2 supports an optional wrapping into ISO/IEC 7816-4 APDUs of the native command set available after ISO/IEC 14443-4 activation for all security levels (including Proximity Checking, see Proximity Check). On top, the following standard ISO/IEC 7816-4 commands are supported for Virtual Card Selection, as defined and described in Virtual Card Architecture:

- ISOSelect with INS code A4h
- ISOExternalAuthenticate with INS code 82h

8.3 Security level switching

There are three security levels of the product:

- SL0: initial delivery configuration, user for card personalization
- SL1: 3-Pass CRYPTO1 Authentication (MIFARE Classic EV1 backwards compatibility mode) with optional AES authentication, optional 3-Pass AES Authentication and secure messaging and the configuration block to restrict update operations (e.g. increment, decrement and/or data write) for DaVaBlocks and Sector Trailers.
- SL3: 3-Pass Authentication based on AES, new data manipulation commands secured by encryption and an AES-based MACing method

Security level switching can be done for the whole card (CardSecurityLevel) or for dedicated sectors only (SectorSecurityLevel). In case of dedicated sectors, these can also be switched to a SL1SL3MixMode, where both SL1 and SL3 operations are accepted. Security level switching, both at card or at sector level, is only possible to a higher security level and not to a lower security level. The added feature in SL1 allows to restrict update operations (e.g. increment, decrement and/or data write) for DaVaBlocks and Sector Trailers in the MIFARE Classic backwards compatibility mode in SL1, see SL1 Update Restrictions.

In case dedicated sectors have been migrated to higher security levels, the overall PICC behavior remains by default according to lowest security level of one of its sectors. By default, the PICC also uses the ATQA/SAK of the lowest security level during the ISO/IEC 14443-3 activation, if these are different for the different security levels. These parameters can be switched to indicate the higher security level before the PICC is completely migrated to a higher security level by means of a configuration option (see MFPConfigurationBlock). Once all sectors are switched to a certain security level, the overall PICC is automatically switched to this security level.

8.4 Security level 0 - SL0

SL0 is the initial delivery configuration of the PICC. The card activation as well as the protocol can be performed in one of the following two ways:

- ISO/IEC 14443-3 (see Section 8.2.1)
- ISO/IEC 14443-4

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

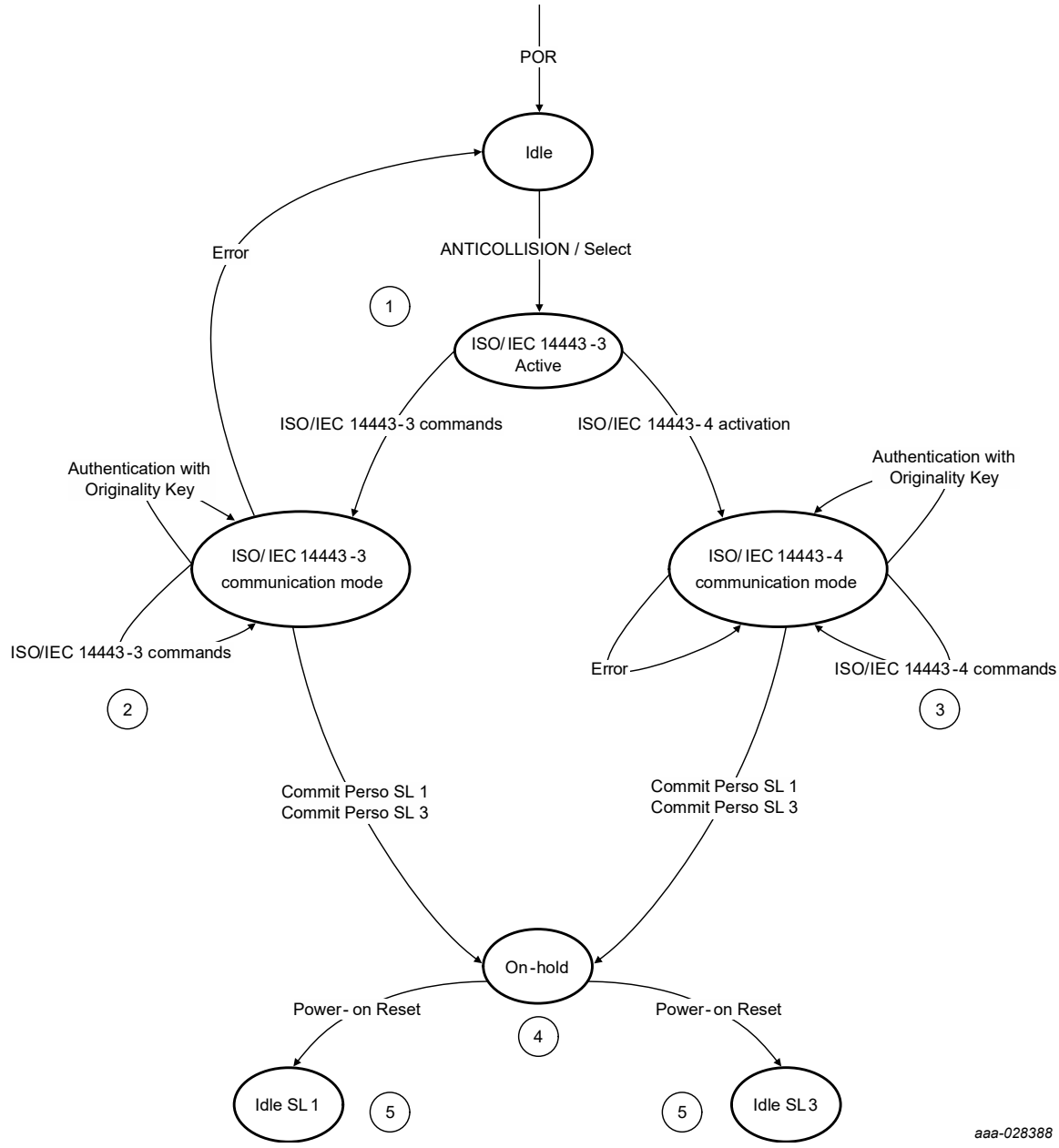


Figure 11. SL0 State Diagram

1. After the anti-collision loop (CL1 for 4BNUID and CL1 + CL2 for 7BUID) the PICC can be activated)
2. With ISO/IEC 14443-3 commands, it is possible to pre-personalize the PICC.
3. Alternatively it is possible to pre-personalize the PICC using ISO/IEC 14443-4 commands. In both communication layers, it is possible to verify the authenticity of the PICC with the authentication OriginalityKey1.
4. When the pre-personalization of the PICC is finished it is possible to upgrade the PICC from SL0 either to SL1 or directly to SL3 with CommitPerso command (see CommitReaderID)
5. A reactivation is needed to activate the PICC to SL1 or SL3.

The following mandatory AES keys must be written using the WritePerso command (see WritePerso) before the PICC can be switched to SL1 or SL3. Security level switching is performed the CommitPerso command (see CommitPerso):

- CardConfigurationKey
- CardMasterKey
- L3SwitchKey (not necessary if card is directly switched to SL3 with the CommitPerso command)

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

8.5 Security level 1 - SL1

SL1 offers the same functionality as a MIFARE Classic EV1 1K/4K using the SL1 backwards compatibility mode. The MIFARE Classic EV1 1K/4K products are specified in [2] and [3]. The protocol is also used in the same way as in the MIFARE Classic EV1 1K/4K (see Section 8.2.1). Furthermore, an additional optional AES authentication is available in this level without affecting the MIFARE Classic 1K/4K functionality. The authenticity of the card can be proven using strong cryptographic means with this additional functionality.

Response timings may differ to the MIFARE Classic EV1 1K/4K products.

In addition to the backwards compatibility mode, after a successful ISO/IEC 14443-4 activation the originality function can be executed or the CardSecurityLevel or SectorSecurityLevel switched to higher security levels. In addition, the same features as available in the previous MIFARE Plus versions. Since MIFARE Plus EV1 the possibility is offered to update AESSectorKeys and VCSystemData. The behavior in SL1 is explained based on the state diagram shown in Figure 12.

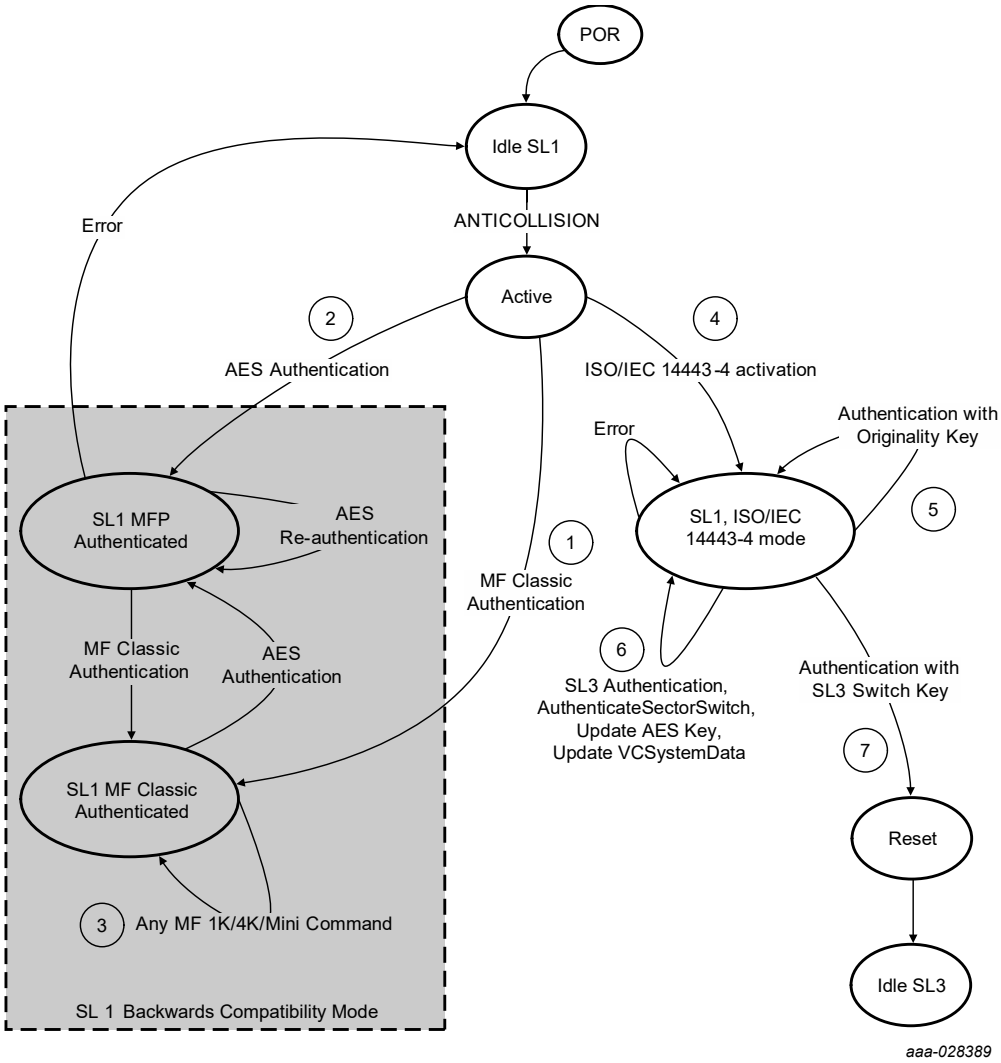


Figure 12. SL1 State Diagram

After an anti-collision loop the card can be, similar as in SL0, put either to backwards compatibility mode or an ISO/IEC 14443-4 mode.

1. Identically as in MIFARE Classic 1K/4K, a CRYPTO1 authentication activates the MF Classic authenticated state.
2. Alternatively, an AES authentication with the SL1CardAuthKey (see Key and block number overview) it is possible to move to SL1 MFP authenticated state. Here a CRYPTO1 authentication is also possible. As shown in the state diagram, the AES authentication is optional and can be performed anytime in the backwards compatibility mode. An AES authentication moves the PICC to the SL1 MFP Authenticated state, meaning the CRYPTO1 authentication has to be repeated in order to access the data again. Keys for AES and CRYPTO1 authentication are not cryptographically bound.
3. In the state SL1 MF Classic Authenticated, the MF1P(H)x2 behaves as MIFARE Classic EV1 1K/4K, see [2] and [3], with the possibility of an optional AES authentication.

4. A full card activation to ISO/IEC 14443-4 is needed to ...
   4.1
   Authenticate with the OriginalityKey1 or ...
   4.2
   Perform full SL3 authentication and secure messaging for sectors which are switched to SL3 SectorSecurityLevel or to SL1SL3Mix mode or update AES keys or VCSystemData or ...
   4.3
   Authenticate with the L3SwitchKey. The authentication can be done both as AuthenticateFirst or AuthenticateNonFirst. Respective Keys as described in Key and block number overview have to be used. After authentication with L3SwitchKey a reset and card activation are needed to start operating in the SL3.

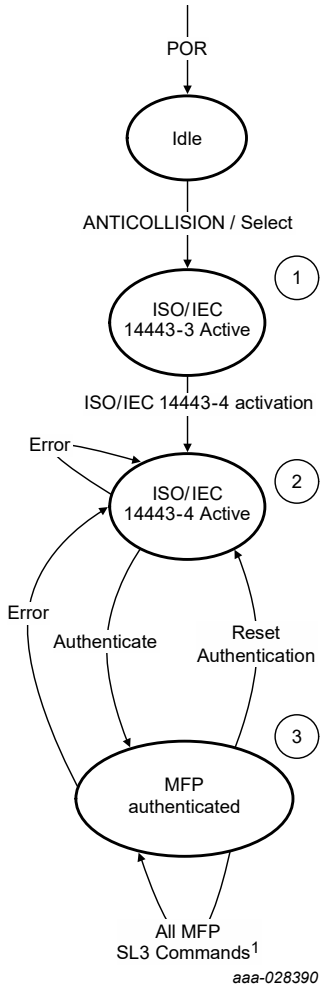
MIFARE Plus EV2 can be operated like previous MIFARE Plus products in SL1, which means that all memory operations on each sector are requiring legacy MIFARE Classic EV1 commands using CRYPTO1 enciphering. In SL1, update operations can be restricted with the configuration block for DaVaBlocks and Sector Trailers to restrict e.g. increment operations. Since release of MIFARE Plus EV1, the flexibility is offered to either switch distinct sectors to SL3 and operate them in AES secure messaging or enable SL1SL3MixMode on distinct sectors. Sectors in SL1SL3MixMode can be operated either using the backwards compatible MIFARE Classic EV1 commands when activated to ISO/IEC 14443-3 or using AES secure messaging when activated to ISO/IEC 14443-4. In example, this enables end-to-end communication to a MIFARE Plus EV2 using a secure AES channel while leaving the operation in the application on MIFARE Classic EV1 commands for a migration period.

Remark: The possibility to activate the MF1P(H)x2 in ISO/IEC 14443-4 can be prevented by using the SetConfigSL1 command, see SetConfigSL1. This feature can be used to satisfy legacy infrastructure requirements.

8.6 Security level 3 - SL3

The operation in SL3 is solely based on the ISO/IEC 14443-4 protocol layer. The usage of the communication in layer 3 backward compatible to MIFARE Classic is not possible anymore. After the activation to ISO/IEC 14443-4, the authentication in any sector can be done only with AES keys while CRYPTO1 based operations are not possible anymore. In SL3 confidentiality and integrity are secured by two separate session keys.

As shown in the simplified state diagram in Figure 13, the PICC has to be first activate in layer 3 mode (state 1) then in layer 4 (state 2). In the MFP authenticated state (state 3), all MFP commands are possible.



1. In this simplified model, VC and Proximity Check commands are not included

Figure 13. SL3, simplified without Virtual Card Architecture and Proximity Check

In SL3, an AES authentication between PICC and reader is conducted, where two keys are generated as a function of the random numbers of the PICC as well as the reader and the shared key. These two unpredictable keys are exclusively used to secure the data which is exchanged on the interface between the card and reader. One of the two keys is used to ensure the confidentiality of the command and response while the other key ensures the integrity of the command and response.

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

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

Other commands, like write commands, 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 (see Integrity) 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 AuthenticateFirst or AuthenticateNonFirst command.

Note that in the case of using a MAC for assuring correct execution of write commands or value operations used within more than one session, the assurance that can be obtained depends on the keys used in this and all of the preceding sessions.

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 SL0, SL1, SL3: ISO/IEC 14443-3 commands

Table 8. ISO/IEC 14443-3 commands

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

9.2 SL0, SL1, SL3: ISO/IEC 14443-4 commands

Table 9. ISO/IEC 14443-4 commands

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 to individually set the communication baud rate independently for both directions.
DESELECT	de-selection according to ISO/IEC 14443-4.

Please also see [5] as well as on the settings of ATQA, SAK and ATS in [4].

9.3 SL0 command overview

Table 10. SL0 command overview

Command	HEX Code	Description
Commands available after ISO/IEC 14443-3 activation		
Read_Sig	3Ch	Retrieve the ECC originality check signature.
WritePerso	A8h	pre Personalization of AES Keys and all blocks
CommitPerso	AAh	switch to SL1 or SL3
AuthenticateFirst (part 1)	70h / 73h	first authenticate
AuthenticateNonFirst (part 1)	76h	following authenticate
AuthenticateContinue (part 2)	72h	second authentication step
VCSupportLastISOL3	4Bh	check if the Virtual Card Concept is supported, communicate PCD capabilities and retrieve the UID
Commands available after ISO/IEC 14443-4 activation		

Table 10. SL0 command overview...*continued*

Command	HEX Code	Description
GetVersion	60h	returns manufacturing related data of the PICC
Read_Sig	3Ch	Retrieve the ECC originality check signature.
WritePerso	A8h	pre Personalization of AES Keys and all blocks
CommitPerso	AAh	switch to SL1 or SL3
AuthenticateFirst (part 1)	70h / 73h	first authenticate
AuthenticateNonFirst (part 1)	76h	following authenticate
AuthenticateContinue (part 2)	72h	second authentication step
VC commands available after ISO/IEC 14443-4 activation, using ISO/IEC 7816-4 protocol		
ISOSelect	A4h	Select virtual card

9.4 SL1 command overview

Table 11. SL1 command overview

Command	HEX Code	Description
MIFARE Classic commands		
MF Authenticate KeyA	60h	authentication with KeyA
MF Authenticate KeyB	61h	authentication with KeyB
MF Read	30h	reading data
MF Write	A0h	writing data
MF Increment	C1h	incrementing a value
MF Decrement	C0h	decrementing a value
MF Restore	C2h	restoring a value
MF Transfer	B0h	transferring a value
Commands using backwards compatibility protocol, see Section 8.2.1.		
Read_Sig	3Ch	Retrieve the ECC originality check signature.
SetConfigSL1	44h	used to change MIFARE Plus EV1 specific configuration data.
MF_PersonalizeUIDUsage	40h	Personalize UID Usage as described in [2]
AuthenticateFirst (part 1)	70h / 73h	first authenticate, protocol used as described in Section 8.2.1
AuthenticateNonFirst (part 1)	76h	following authenticate, protocol used as described in Section 8.2.1
AuthenticateContinue (part 2)	72h	second authentication step, protocol used as described in Section 8.2.1
ReadPlainNoMAC_UnMACed	36h	reading in plain, no MAC on response, no MAC on command

Table 11. SL1 command overview...*continued*

Command	HEX Code	Description
VCSupportLastISOL3	4Bh	check if the Virtual Card Concept is supported, communicate PCD capabilities and retrieve the UID
Authentication commands available after ISO/IEC 14443-4 activation [1]		
GetVersion	60h	returns manufacturing related data of the PICC
Read_Sig	3Ch	Retrieve the ECC originality check signature.
AuthenticateFirst (part 1)	70h / 73h	first authenticate
AuthenticateNonFirst (part 1)	76h	following authenticate
AuthenticateSectorSwitch (part 1)	7Ah	used to switch single sectors to SL3, see AuthenticateSectorSwitch
AuthenticateContinue (part 2)	72h	second authentication step
ResetAuth	78h	reset the authentication
Memory commands available after ISO/IEC 14443-4 activation [2]		
WriteEncryptedNoMAC	A0h	writing encrypted, no MAC on response, MAC on command
WriteEncryptedMAC	A1h	writing encrypted, MAC on response, MAC on command
Proximity check commands available after ISO/IEC 14443-4 activation		
PreparePC	F0h	prepare for the Proximity Check
ProximityCheck	F2h	perform the precise measurement for the proximity check
VerifyPC	FDh	verify the proximity check
VC commands available after ISO/IEC 14443-4 activation, using ISO/IEC 7816-4 protocol		
ISOSelect	A4h	Select virtual card
ISOExternalAuthenticate	82h	Authenticate PD

[1] for security level switch, the originality function, sector security level switch and updating of AES keys and VCSystemData blocks

[2] for updating of AES keys and VCSystemData blocks

In addition to the commands listed in Table 11, all commands defined for SL3 communication are available for those sectors which have been switch to SL3 or SL1SL3Mix mode using the AuthenticateSectorSwitch feature.

9.5 SL3 command overview

Table 12. SL3 command overview

Command	HEX code	Description
MIFARE Plus commands		
GetVersion	60h	returns manufacturing related data of the PICC

Table 12. SL3 command overview*...continued*

Command	HEX code	Description
Read_Sig	3Ch	Retrieve the ECC originality check signature.
AuthenticateFirst (part 1)	70h / 73h	first authenticate
AuthenticateNonFirst (part 1)	76h	following Authenticate
AuthenticateContinue (part 2)	72h	second authentication step
ResetAuth	78h	reset the authentication
Additional Frame	AFh	proceed to next response frame in GetVersion
READ commands		
ReadEncryptedNoMAC_MACed	30h	reading encrypted, no MAC on response, MAC on command
ReadEncryptedMAC_MACed	31h	reading encrypted, MAC on response, MAC on command
ReadPlainNoMAC_MACed	32h	reading in plain, no MAC on response, MAC on command
ReadPlainMAC_MACed	33h	reading in plain, MAC on response, MAC on command
ReadEncryptedNoMAC_UnMACed	34h	reading encrypted, no MAC on response, no MAC on command
ReadEncryptedMAC_UnMACed	35h	reading encrypted, MAC on response, no MAC on command
ReadPlainNoMAC_UnMACed	36h	reading in plain, no MAC on response, no MAC on command
ReadPlainMAC_UnMACed	37h	reading in plain, MAC on response, no MAC on command
WRITE commands		
WriteEncryptedNoMAC	A0h	writing encrypted, no MAC on response, MAC on command
WriteEncryptedMAC	A1h	writing encrypted, MAC on response, MAC on command
WritePlainNoMAC	A2h	writing in plain, no MAC on response, MAC on command
WritePlainMAC	A3h	writing in plain, MAC on response, MAC on command
VALUE operations		
IncrementNoMAC	B0h	incrementing a value encrypted, no MAC on response, MAC on command
IncrementMAC	B1h	incrementing a value encrypted, MAC on response, MAC on command
DecrementNoMAC	B2h	decrementing a value encrypted, no MAC on response, MAC on command

Table 12. SL3 command overview*...continued*

Command	HEX code	Description
DecrementMAC	B3h	decrementing a value encrypted, MAC on response, MAC on command
TransferNoMAC	B4h	transferring a value, no MAC on response, MAC on command
TransferMAC	B5h	transferring a value, MAC on response, MAC on command
IncrementTransferNoMAC	B6h	combined incrementing and transferring a value encrypted, no MAC on response, MAC on command
IncrementTransferMAC	B7h	combined incrementing and transferring a value encrypted, MAC on response, MAC on command
DecrementTransferNoMAC	B8h	combined decrementing and transferring a value encrypted, no MAC on response, MAC on command
DecrementTransferMAC	B9h	combined decrementing and transferring a value encrypted, MAC on response, MAC on command
RestoreNoMAC	C2h	restoring a value, no MAC on response, MAC on command
RestoreMAC	C3h	restoring a value, MAC on response, MAC on command
Proximity check commands		
PreparePC	F0h	prepare for the Proximity Check
ProximityCheck	F2h	perform the precise measurement for the proximity check
VerifyPC	FDh	verify the proximity check
VC commands using ISO/IEC 7816-4 protocol		
ISOSelect	A4h	Select virtual card
ISOExternalAuthenticate	82h	Authenticate PD
Transaction MAC commands		
CommitReaderID	C8h	commit reader ID for Transaction MAC

10 Limiting values

Table 13. Limiting values
[1] [2]

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

Symbol	Parameter	Conditions	Min	Max	Unit
$P_{d,max}$	maximum power dissipation		-	240	mW
$I_{LA-LB,max}$	maximum input current at the antenna pads LA/LB		-	86	mA
T_{stg}	storage temperature		-55	125	°C
T_{amb}	ambient temperature		-25	85	°C
V_{ESD}	electrostatic discharge voltage on LA/LB	human body model (HBM)[3], C = 100 pF, R = 1.5 kΩ	-	4	kV

[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] According to ANSI/ESDA/JEDEC JS-001.

CAUTION

This device is sensitive to ElectroStatic Discharge (ESD). Observe precautions for handling electrostatic sensitive devices.
Such precautions are described in the *ANSI/ESD S20.20, IEC/ST 61340-5, JESD625-A* or equivalent standards.

11 Abbreviations

Table 14. Abbreviations

Acronym	Description
AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
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
SL	Security level
UID	Unique IDentifier
VC	Virtual Card, one MIFARE Plus PICC is one virtual card
WUPA	Wake Up Protocol A

12 References

[1]

MF1P(H)x2 Wafer specification

Data sheet addendum, BU S&C Doc. No. 3441** [3]

[2]

MIFARE Classic EV1 1K

Product data sheet, MF1S50YYX_V1 MIFARE Classic EV1 1K - Mainstream contactless smart card IC for fast and easy solution development, https://www.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf

[3]

MIFARE Classic EV1 4K

Product data sheet, MF1S70YYX_V1 MIFARE Classic EV1 4K - Mainstream contactless smart card IC for fast and easy solution development , https://www.nxp.com/docs/en/data-sheet/MF1S70YYX_V1.pdf

[4]

AN10833 MIFARE Type Identification Procedure

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

[5]

AN10834 ISO 14443 PICC Selection

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

[6]

AN10922 Symmetric key diversifications

Application note, https://www.nxp.com/docs/en/application-note/AN10922.pdf

[7]

AN4462 MIFARE Plus EV2 Originality Signature Validation

Application note, BU S&C Doc.No. 4462**[3]

[8]

ISO/IEC 14443-3:2018

Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 3: Initialization and anti-collision.

[9]

ISO/IEC 14443-4:2018

Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 4: Transmission protocol.

[10]

ISO/IEC 7816-4:2013

3 ** ... DocStore document version number

Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange.

[11]

ISO/IEC 7816-5:2004

Identification cards – Integrated circuit cards – Part 5: Registration of application providers.

[12]

ISO/IEC 9797-1:2011

Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher.

[13]

DATA ENCRYPTION STANDARD

National Institute of Standards and Technology (NIST). Federal Information Processing Standards Publication 46-3, October 1999.

[14]

Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher

National Institute of Standards and Technology (NIST). NIST Special Publication 800-67, May 2004.

[15]

Specification for the Advanced Encryption Standard (AES)

National Institute of Standards and Technology (NIST). Federal Information Processing Standards Publication 197, November 2001.

[16]

Recommendation for Block Cipher Modes of Operation: Methods and Techniques

National Institute of Standards and Technology (NIST). NIST Special Publication 800-38A, December 2001.

[17]

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

National Institute of Standards and Technology (NIST). NIST Special Publication 800-38B, May 2005.

[18]

Recommendation for key derivation using pseudorandom functions

National Institute of Standards and Technology (NIST). NIST Special Publication 800-108, November 2008.

[19]

AN10927 MIFARE product and handling of UIDs

Application note, https://www.nxp.com/docs/en/application-note/AN10927.pdf

[20]

AN11909 How to create an Installation IDentifier (IID)

Application note, https://www.nxp.com/docs/en/application-note/AN11909.pdf

[21]

Global Platform card specification

Globalplatform. Version 2.2.1, January 2011

[22]

Global Platform - contactless services

Globalplatform card - contactless services - card specification. v2.2 - Amendment C, Version 1.1, April 2013

[23]

Sun Microsystems

Java card http://www.oracle.com/technetwork/java/javacard/overview/index.html.

[24]

Contactless smart card module specification MOA4

Delivery Type Description, BU S&C Doc.No. 0823**[3]

[25]

Contactless smart card module specification MOA8

Delivery Type Description, BU S&C Doc.No. 1636**[3]

[26]

General specification for 12" wafer on UV-tape; delivery types

Delivery Type Description, BU S&C Doc.No. 1862**[3]

[27]

Certicom Research. Sec 1:

Elliptic curve cryptography. Version 2.0, May 2009.

[28]

Certicom Research. Sec 2:

Recommended elliptic curve domain parameters. Version 2.0, January 2010.

13 Revision history

Table 15. Revision history

Document ID	Release date	Data sheet status	Supersedes
MF1P(H)x2_SDS v.3.1	20210809	Short product data sheet	MF1P(H)x2_SDS v.3.0
Modifications:	• Section 12 "References": updated		
MF1P(H)x2_SDS v.3.0	20200622	Short product data sheet	-
Modifications:	• First release		

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 — 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.

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. 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.

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 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 or documented vulnerabilities. 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.

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.

DESFire — 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.

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

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