P5DF081

MIFARE secure access module SAM AV2

Rev. 3.2 — 17 December 2013
191732

Product short data sheet
COMPANY PUBLIC

1. General description

The NXP MIFARE SAM AV2 hardware solution is the ideal add-on for reader devices offering additional security services. Supporting TDEA, AES and RSA capabilities, it offers secure storage and secure communication in a variety of infrastructures.

Unlike other products in the field, MIFARE SAM AV2 has proven interoperability with all of NXP's broad card portfolio, (MIFARE Ultralight, MIFARE Ultralight C, MIFARE 1K, MIFARE 4K, MIFARE Plus, MIFARE DESFire, MIFARE DESFire EV1 and SmartMX solutions), making it the most versatile and secure SAM solution on the market today.

Secured communication

When used in combination with a reader IC supporting innovative "X" features, MIFARE SAM AV2 provides a significant boost in performance to the reader along with faster communication between reader and module. The "X" feature is a new way to use the SAM in a system, with SAM connected to the microcontroller and the reader IC simultaneously. The one variant, identified with T1AD2060, can be connected to RC52X contactless reader ICs, the other variant, identified T1AR1070, can be connected to RC663 using the X-feature. Apart from the difference in the interface, both variants have the same functionality.

The connection between the SAM and the reader is performed using security protocols based on either symmetric cryptography (TDEA and AES) or PKI RSA asymmetric cryptography. The protocols comply with the state-of-art standards and thereby ensure data confidentiality and integrity.

2. Features and benefits

2.1 Cryptography

- Supports MIFARE Crypto1, TDEA (Triple DES encryption algorithm), RSA and AES cryptography
- Supports MIFARE Ultralight, MIFARE Ultralight C, MIFARE 1K, MIFARE 4K, MIFARE Plus, MIFARE DESFire, MIFARE DESFire EV1
- Secure storage and updating of keys (key usage counters)
- 128 key entries for symmetric cryptography and 3 RSA key entries for asymmetric cryptography
- TDEA and AES based key diversification
- Offline cryptography

2.2 Communication

- Up to four logical channels; simultaneous multiple card support
- Support for DESFire and MIFARE Plus authentication (with related secure messaging and session key generation)
- Secure Host to SAM and back end to SAM communication with symmetric cryptography 3 pass authentication for confidentiality and integrity
- Support high speed baud rates up to 1.5 Mbit/s
- Secure Host to SAM and back end to SAM communication with RSA based cryptography
- Support ISO/IEC 7816 baud rates
- True random number generator (TRNG)

2.3 Delivery types

- Available in wafer, PCM 1.1 module, or HVQFN package

3. Applications

- Access management
- Public transport
- Loyalty programs
- Micro payment

4. Quick reference data

Table 1. Quick reference data

V_{DD}; V_{SS} = 0 V; T_{amb} = −25 °C to +85 °C

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
V_{DD}	supply voltage	Class A: 5 V range	4.5	5.0	5.5	V
		Class B: 3 V range	2.7	3.0	3.3	V

5. Ordering information

Table 2. Ordering information

Type number	Package		
	Name	Description	Version
P5DF081X0/T1AD2060	PCM1.1	contact chip card module (super 35 mm tape format, 8 contact), minimum order quantity: 10.000	SOT658-1
P5DF081X0/T1AD2060S	PCM1.1	contact chip card module (super 35 mm tape format, 8 contact), minimum order quantity: 1.000	SOT658-1
P5DF081HN/T1AD2060	HVQFN32	plastic thermal enhanced very thin quad flat package; no leads; 32 terminals; body 5 x 5 x 0.85 mm	SOT617-3
P5DF081UA/T1AD2060	FCC	sawn wafer 150 mm on film frame carrier	-
P5DF081X0/T1AR1070	PCM1.1	contact chip card module (super 35 mm tape format, 8 contact), minimum order quantity: 10.000	SOT658-1

Table 2. Ordering information *...continued*

Type number	Package		
	Name	Description	Version
P5DF081X0/T1AR1070S	PCM1.1	contact chip card module (super 35 mm tape format, 8 contact), minimum order quantity: 1.000	SOT658-1
P5DF081HN/T1AR1070	HVQFN32	plastic thermal enhanced very thin quad flat package; no leads; 32 terminals; body 5 x 5 x 0.85 mm	SOT617-3
P5DF081UA/T1AR1070	FCC	sawn wafer 150 mm on film frame carrier	-

6. Block diagram

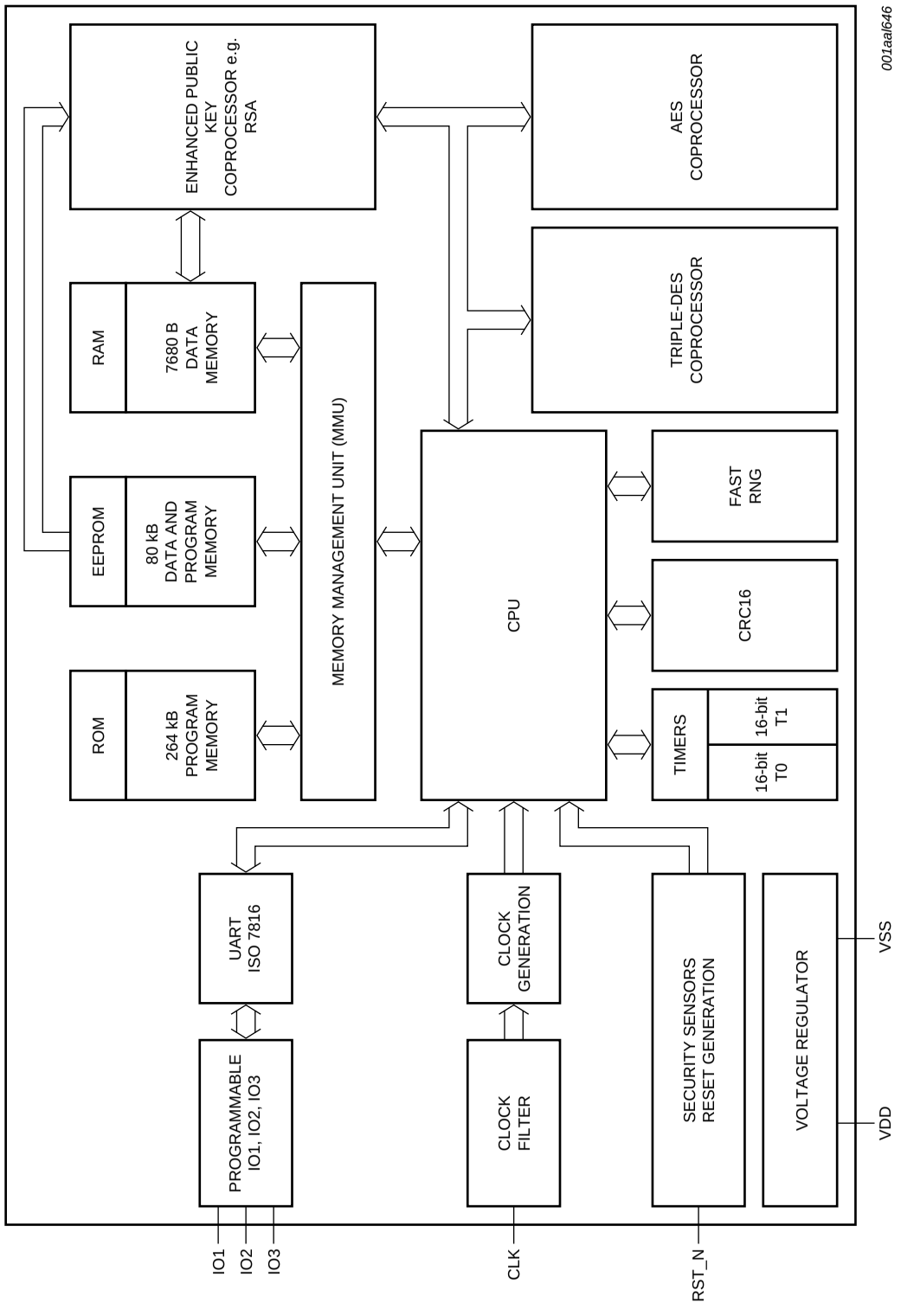


Fig 1. Block diagram

7. Pinning information

7.1 Pinning

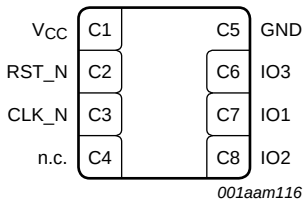
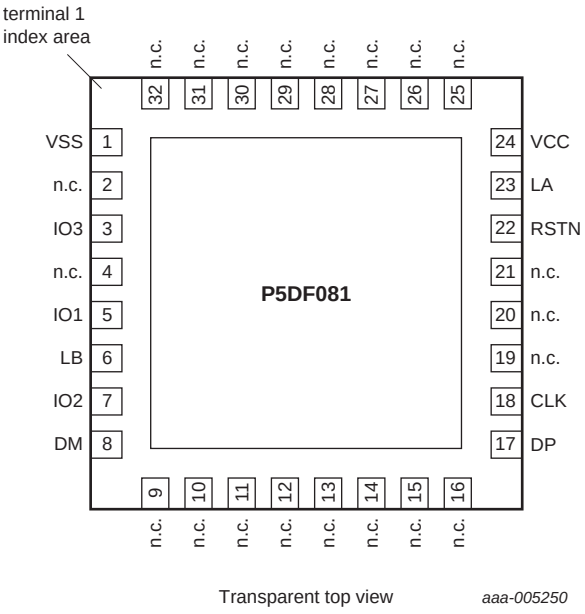


Fig 2. Pin configuration PCM1.1

7.2 Pinning



Remark: Central pad is isolated.

Fig 3. Pin configuration HVQFN32

7.3 Pin description

Table 3. Pin description PCM 1.1 MIFARE SAM AV2

ISO/IEC 7816		MIFARE SAM AV2		
Pad	**Symbol**	**Symbol**	**Pad**	**Description**
C1	VCC	V_{CC}	C1	power supply voltage input
C2	RST	RST_N	C2	reset input, active LOW
C3	CLK	CLK_N	C3	clock input
C4	reserved	n.c.	C4	n.c.

Table 3. Pin description PCM 1.1 MIFARE SAM AV2 *...continued*

ISO/IEC 7816		MIFARE SAM AV2		
Pad	**Symbol**	**Symbol**	**Pad**	**Description**
C5	GND	GND	C5	ground (reference voltage) input
C6	VPP	IO3	C6	used for I2C communication to RC52x or RC663 (SCLK)
C7	IO1	IO1	C7	input/output for serial data (host communication)
C8	reserved	IO2	C8	used for I2C communication to RC52x or RC663

Table 4. Pin description HVQFN32 MIFARE SAM AV2

HVQFN32		MIFARE SAM AV2		
Pad	**Symbol**	**Symbol**	**Pad**	**Description**
1	VSS	GND	1	ground (reference voltage) input
2	n.c.	n.c.	2	not connected
3	IO3	IO3	3	used for I2C communication to RC
4	n.c.	n.c.	4	not connected
5	IO1	IO1	5	input/output for serial data (host communication)
6	LB	n/a	6	not used
7	IO2	IO2	7	used for I2C communication to RC (SDATA)
8	DM	n/a	8	not used
9	n.c.	n.c.	9	not connected
10	n.c.	n.c.	10	not connected
11	n.c.	n.c.	11	not connected
12	n.c.	n.c.	12	not connected
13	n.c.	n.c.	13	not connected
14	n.c.	n.c.	14	not connected
15	n.c.	n.c.	15	not connected
16	n.c.	n.c.	16	not connected
17	DP	n/a	17	not used
18	CLK	CLK_N	18	clock input
19	n.c.	n.c.	19	not connected
20	n.c.	n.c.	20	not connected
21	n.c.	n.c.	21	not connected
22	RSTN	RST_N	22	reset input, active LOW
23	LA	n/a	23	not used
24	VCC	VCC	24	power supply voltage input

8. Functional specification

8.1 Hardware interface

8.1.1 Contact interface

The pad assignment and the electrical characteristics are fully compliant with ISO/IEC 7816 (part 2 and part 3). The MIFARE SAM AV2 operates with Class A and Class B interface devices. An internal charge pump provides the EEPROM programming voltage. Note that pad C6 is not a programming voltage input but is an output line for the clock signal for I2C communication to the RC52x or RC663 reader chip. Pad C8 is used as data line to the reader chip. These two pads for connection to the RC52x or RC663 are the only ones deviating from the ISO standard pin assignment.

8.1.2 External clock frequency and bit rates

The basic operation frequency of the MIFARE SAM AV2 is 3.5712 MHz. With this frequency the following standard bit rates can be reached using ISO/IEC 7816 transmission factors F and D.

The MIFARE SAM AV2 supports significantly higher transmission speeds.

The maximum specified bit rate in any case is 1.5 Mbit/s.

8.1.3 Card operation procedures

All card operation procedures (activation, cold reset, warm reset and deactivation) are fully compliant with Ref. 19, Chapter 5.

8.2 Transmission procedure and communication

8.2.1 Protocol activation sequence

All subsequently described operations are compliant with ISO/IEC 7816-3.

8.2.1.1 Answer To Reset (ATR)

The MIFARE SAM AV2 offers two modes of operation identified by different ATRs.
A negotiable mode where the bit rate has to be adjusted via a PPS request and a specific mode where the MIFARE SAM AV2 switches automatically to F = 128 and D = 32 (highest possible speed) after sending the ATR. Starting with the negotiable mode, the mode of operation is switched after every warm reset.

After a cold reset, the card sends the following ATR to the terminal.

Table 5. ATR after cold reset

Character	Value	Meaning
TS	3Bh	initial character; setting up direct convention
T0	DFh	TA(1), TC(1), TD(1) are present; number of historical characters is 15
TA(1)	18h	F = 372; D = 12
TC(1)	FFh	no extra guard time needed; N = 255
TD(1)	81h	TD(2) is present; protocol T = 1

Table 5. ATR after cold reset *…continued*

Character	Value	Meaning
TD(2)	F1h	TA(3), TB(3), TC(3) and TD(3) are present; protocol T = 1
TA(3)	FEh	Information field size of the card = 254
TB(3)	43h	BWT indicator = 4; CWT indicator = 3
TC(3)	00h	error detection code = LRC
TD(3)	3Fh	TA and TB for T = 15 is present; protocol T = 15 (qualifies global interface bytes)
TA(after T = 15)	03h	clock stop not supported; Class A, Class B
TB(after T = 15)	83h	Proprietary use of C6 (IO3, reception of serial data from RC52x or RC663)
Historical bytes	4Dh, 49h, 46h, 41h, 52h, 45h, 20h, 50h, 6Ch, 75h, 73h, 20h, 53h, 41h, 4Dh	ASCII value of “MIFARE Plus SAM”
TCK	3B	check character

After this ATR, the card is in the negotiable mode and waits for a PPS request. If a warm reset is issued, the MIFARE SAM AV2 switches the mode of operation, enters the specific mode and sends the following ATR.

Table 6. ATR after warm reset

Character	Value	Meaning
TS	3Bh	initial character; setting up direct convention
T0	DFh	TA(1), TC(1) and TD(1) are present; number of historical characters is 15
TA(1)	18h	F = 128 and D = 32
TC(1)	FFh	no extra guard time needed; N = 255
TD(1)	81h	TA(2) and TD(2) are present; protocol T = 1
TA(2)	F1h	specific mode byte: capable of changing the mode of operation; parameters defined by interface bytes; protocol T = 1
TD(2)	FEh	TA(3), TB(3), TC(3), TD(3) are present; protocol T = 1
TA(3)	43h	information field size of the card = 254
TB(3)	00h	BWT indicator = 4; CWT indicator = 3
TC(3)	3Fh	error detection code = LRC
TD(3)	07h	TA and TB for T = 15 is present, protocol T = 15 (qualifies global interface bytes)
TA(after T = 15)	83h	clock stop not supported, Class A and Class B
TB(after T = 15)	18h	Proprietary use of C6 (IO3, reception of serial data from RC52x or RC663)
Historical bytes	4Dh, 49h, 46h, 41h, 52h, 45h, 20h, 50h, 6Ch, 75h, 73h, 20h, 53h, 41h, 4Dh	ASCII value of “MIFARE Plus SAM”
TCK	98h	check character

After every future warm reset, the mode of operation and therefore also the ATR is toggled with the ATR after cold reset.

8.2.1.2 Protocol and Parameter Selection (PPS exchange)

The PPS command allows to individually select the transmission factors and the communication protocol.

The PPS was successful if the response exactly echoes the request.

8.2.2 Protocol T = 1

The MIFARE SAM AV2 offers a T = 1 protocol which is fully compliant with *ISO/IEC 7816-3, Chapter 9*.

For details on how to calculate the resulting time-outs, refer to *ISO/IEC 7816-3, Chapter 9.5*.

8.2.3 APDU structure

All instructions sent to the MIFARE SAM AV2 have to be coded into an APDU structure according to ISO/IEC 7816-4 and inserted into the information field of one or more I-Blocks.

The commands do not belong to the inter-industry class. The coding of the command and response pairs is proprietary, only the structure is compliant with ISO/IEC 7816-4.

8.2.4 UID/serial number

The MIFARE SAM AV2 IC features a 7 byte unique serial number that is programmed into a locked part of the non-volatile memory that is reserved for the manufacturer. This UID is fixed and cannot be changed.

8.3 MIFARE SAM AV1 compatibility mode vs. MIFARE SAM AV2 mode

Unless stated explicitly otherwise, all information in this document refer to both the MIFARE SAM AV1 compatibility mode and to the pure MIFARE SAM AV2 mode. Commands only available in pure MIFARE SAM AV2 mode are flagged as "AV2 only". Differences for commands different in SAM AV2 with respect to their corresponding SAM AV1 compatibility version are listed explicitly as well.

The main differences between the AV1 compatibility mode and the AV2 mode are the following:

- PKI commands are only available in AV2 mode
- AV2 mode introduces key classes: Host Keys, PICC keys, OfflineChange keys and OfflineCrypto keys. All symmetric key entries are classified into one of them, restricting the possible usage of the key entry.
- AV2 mode improves the SAM access protection by replacing the AV1 compatibility Host Authentication protocols with more secure variants.
- AV2 mode improves the SAM-Host communication protection by replacing the AV1 compatibility increased security mode (based on CMACing) by three modes of secure messaging after a host authentication (Plain, MAC Protection and Full Protection).
- AV2 mode replaces and adds some key entry configuration options, offering more flexibility in securing the SAM (e.g. regarding key dumping).

8.4 Cryptography and key handling

8.4.1 Cryptography

AV1 compatibility mode supports symmetric key cryptographic algorithms while MIFARE SAM AV2 mode supports both symmetric and asymmetric cryptography.

8.4.1.1 Symmetric key cryptography

MIFARE SAM AV2 offers support in several commands for various symmetric key cryptographic algorithms.

DES and TDEA

DES keys (56 bit) and 2TDEA keys (112 bit) are stored in 16 byte strings. 3TDEA keys (168 bits) are stored in 24 byte strings.

DES keys (56 bit) are stored in the same format as the 2TDEA keys: the DES key is stored twice to form a 2 key TDEA key where the 2 keys are identical.

AES

AES keys are stored in strings of 16 bytes or 24 bytes depending on whether it is an AES 128-bit key or an AES 192-bit key.

AES always operates on 16 bytes. Therefore data streams are always padded to a length of multiples of 16 bytes.

For details of the AES standard please refer to publicly available standard (Ref. 31).

AES MACing

MIFARE SAM AV2 supports standard CMAC [ref. 15] for AES. Padding is done according to the standard. By default, the CMAC is truncated to 8 bytes, except if requested explicitly otherwise by the user (SAM_Generate_MAC and SAM_Verify_MAC commands).

An alternate MAC truncation scheme is used for MIFARE Plus commands for the AV2 mode SAM-Host communication protection and possible via SAM_Generate_MAC and SAM_Verify_MAC commands.

MIFARE Classic

MIFARE SAM AV2 supports MIFARE Classic Crypto-1 authentication and encryption.

8.4.1.2 Asymmetric key cryptography (MIFARE SAM AV2 mode only)

MIFARE SAM AV2 supports RSA encryption, decryption, signature generation and signature verification according to Ref. 16. These algorithms are available in AV2 mode via the PKI commands.

RSA encryption and decryption: The PKI functionalities of the MIFARE SAM AV2 support RSA decryption. It is used by the PKI_UpdateKeyEntries command. The supported algorithm is RSAES-OAEP Ref. 16 The OAEP padding requires a hashing function and a Mask Generation Function (MGF). For the MGF, the SAM supports SHA-1, SHA-224 and SHA-256 for hashing (see Ref. 9 for the various SHA variants); the MGF used is the one specified by (Ref. 17 §B.2.1).

RSA signature generation and verification: The PKI functionalities of MIFARE SAM AV2 support RSA signature handling. It is used by the PKI_GenerateSignature, PKI_VerifySignatures and PKI_UpdateKeyEntries commands. The supported algorithm is RSASSA-PSS (see Ref. 16). The PKI_GenerateSignature and PKI_VerifySignatures commands expect the already hashed message mHash as input. The initial hash operation (Step 1 and 2 of EMSA-PSS-Encode and EMSA-PSS-Verify, Ref. 16) is not calculated by this function.

Hashing algorithms (MIFARE SAM AV2 only): MIFARE SAM AV2 supports SHA-1, SHA-224 and SHA-256 for hashing according to Ref. 17. These hashing algorithms are available in AV2 mode via the PKI_GenerateHash command.

8.4.2 Key diversification

MIFARE SAM AV2 provides several key diversification methods. In both AV1 compatibility mode and in MIFARE SAM AV2 mode, the MIFARE SAM AV1 key diversification methods and new MIFARE SAM AV2 key diversification methods are available; however for AV2 only commands (i.e. MFP commands and the ULC_AuthenticatePICC) only the new MIFARE SAM AV2 diversification methods are available.

8.4.3 Key Storage (MIFARE SAM AV1 compatibility mode)

MIFARE SAM AV2 in AV1 compatibility mode can only store symmetric keys.

MIFARE SAM AV2 can store up to 128 symmetric keys in up to 3 versions (only 2 versions possible for 3TDEA keys and AES-192 keys).

8.4.3.1 Symmetric keys

The MIFARE SAM AV2 uses a Key Storage Table (KST) in order to store and manage keys and attributes related to keys.

The KST holds 128 entries. Every entry contains positions to store three DES, three 2TDEA, two 3TDEA, three AES128, two AES192 or six MIFARE keys plus their attributes.

Every key entry is referred to by its index, the KeyNo.

Key reference number: KeyNo is the index of the entry in the KST and can have the value 00h to 7Fh.

Key reference number of change entry key: The 1-byte field holds the KeyNo that is necessary for authentication to run a SAM_ChangeKeyEntry command.

The value FEh disables the need for authentication for key load.

The value FFh irreversibly locks the entire key entry.

Key version of change entry key: The 1-byte field holds the key version within the key entry specified for the change entry key. The key version has to be in the range of 00h to FFh.

Reference number of key usage counter: The 1-byte field holds the reference number of the key usage counter entry which is automatically incremented each time this key entry is used for authentication, see Section 8.4.6.

8.4.4 Key Storage (MIFARE SAM AV2 mode)

MIFARE SAM AV2 in MIFARE SAM AV2 mode can store both symmetric and asymmetric keys.

8.4.4.1 Symmetric keys

MIFARE SAM AV2 can store up to 128 symmetric keys in up to 3 versions (only 2 versions possible for 3TDEA keys and AES-192 keys) There only difference in the content of a key entry compared to AV1 compatibility mode is the addition of an ExtSET byte with extended configuration settings, as can be seen in Table 14.

Storage and configuration options: Next to the addition of the ExtSET byte, part of the SET configuration settings got redefined when comparing AV2 mode to the AV1 compatibility mode.

Four classes of keys are distinguished which restrict the possible usage of a key entry to part of the SAM functionality:

1. Host Keys: used for protecting the SAM-Host communication (see Section 8.5) These keys are restricted to the AES key types.
2. PICC Keys: used for the card communication; depending on the key type they can be used for authenticating and communicating with a MIFARE Plus, DESFire, MIFARE Classic and/or MIFARE Ultralight C card
3. OfflineChange Keys: used for some key management commands, to allow offline preparation of the cryptograms for these commands (compared to when the key management is done with Host Keys) These keys are restricted to the AES key types.
4. OfflineCrypto Keys: used for offline crypto operations: e.g. for communication with the backend or for writing encrypted data on a MIFARE Plus Slim or MIFARE Ultralight (C) card.

Note that the key classes are mutual exclusive: one key cannot belong to more than 1 of these classes.

KST reset when activating MIFARE SAM AV2 mode: From MIFARE SAM AV2 mode on, the keys stored in the KST are identified as Host, PICC, OfflineChange or OfflineCrypto Keys. For this reason the KST is reset when activating MIFARE SAM AV2 mode, as it is not clear how to assign the existing keys to one of the classes automatically.

8.4.4.2 Asymmetric keys

MIFARE SAM AV2 can store 2 RSA public key pairs and one RSA public key.MIFARE SAM AV2 supports RSA keys with a modulus with a size from 256 bit (i.e. 32 bytes) up to 2048 bit (i.e. 256 bytes).

PKI Key Storage Table: MIFARE SAM AV2 uses a PKI Key Storage Table (PKI_KST) in order to store and manage RSA asymmetric key pairs (i.e. private and public keys) and the attributes related to keys. The PKI_KST holds 3 entries.

8.4.5 Key versioning

The MIFARE SAM AV2 reserves three bytes in a key entry to store the version of the three available keys in the entry. This version byte contains the key version for all kinds of keys (DES, TDEA, AES and MIFARE). The version information must be included separately in every key entry of type AES or MIFARE when it is updated by the ChangeKeyEntry command.

8.4.6 Key usage counters

In order to count and limit the number of authentications a key entry can be used for, MIFARE SAM AV2 stores a table of 16 key usage counter entries, 00h to 0Fh, which are automatically incremented each time a defined key entry is used for authentication. Multiple key entries can use the same counter.

8.4.6.1 Reference number

The property RefNoKUC codes the reference number of the key usage counter. RefNoKUC is the index of the entry in the table and can have the value 00h to 0Fh, therefore 16 key usage counters can be stored.

8.4.6.2 Limit

This field stores the current limit for this key usage counter. It is only possible to use a key that is linked to this counter for authentication if the current value (see below) is smaller than the current limit. As soon as the current value is equal to, or higher than, the current limit, the usage of all key entries linked to this counter is prohibited.

8.4.6.3 Key reference number to change the current KUC entry

In order to change the KUC, a successful authentication by the host application of the MIFARE SAM AV2 is necessary. The KeyNoCKUC defines the reference number of the KST which is used for this.

8.4.6.4 Key version to change the current KUC entry

The 1-byte field holds the key version within the key entry specified to change the KUC entry. The key version has to be in the range of 00h to FFh. The MIFARE SAM AV2 will automatically select the appropriate key from one of three positions in the entry that has the specified version number.

8.4.6.5 Current value

The CurVal field stores the current value of this key usage counter. It is possible to use all keys referring to this counter for authentication only if the current value is smaller than the current limit.

8.5 SAM - Host communication

8.5.1 General principles for SAM-Host protection

MIFARE SAM AV2 supports two different modes: AV1 compatibility mode and MIFARE SAM AV2 mode. A MIFARE SAM AV2 is initially in MIFARE SAM AV1 compatibility mode. It can be switched to the MIFARE SAM AV2 by executing a host authentication with the SAM Master Key using the SAM_LockUnlock command. Note that MIFARE SAM AV2 mode activation is thus only possible if the SAM Master Key is configured as an AES128

or AES192 key. During this activation authentication, the maximal message size under command chaining (MaxChainBlocks) is set. Once switched to MIFARE SAM AV2 mode there is no mean to switch back.

When the MIFARE SAM AV2 mode is activated, the Key Storage Table (except the SAM Master Key) gets reset.

8.5.2 MIFARE SAM AV1 compatibility mode SAM-Host protection

In AV1 compatibility mode, SAM access and SAM-Host communication is protected by the increased security mode exactly like for the MIFARE SAM AV1. The protection mechanism is explained in the following subsection.

8.5.2.1 Increased security - CMAC calculation

The MIFARE SAM AV2 offers the possibility to send each command on a higher security level by applying a CMAC. If activated, the MIFARE SAM AV2 requires a logical channel with an active host authentication to be defined for CMAC calculation to accept any command.

The CMAC is calculated and padded according to the NIST Special Publication 800-38B, which gives a recommendation for block cipher modes of operation.

The following commands of the MIFARE SAM AV2 do not apply the explained CMAC mechanism:

- SAM_AuthenticateHost
- SAM_GetChallenge, SAM_InternalAuthenticate and SAM_ExternalAuthenticate

Commands already protected by encryption apply the explained CMAC mechanism only for the direction which is not protected:

- SAM_ChangeKeyEntry for the command APDU
- SAM_ChangeKUCEntry for the command APDU
- SAM_DumpSessionKey for the response APDU
- SAM_ChangeKeyMIFARE for the response APDU

8.5.3 MIFARE SAM AV2 mode SAM-Host protection

Two kinds of host authentication can be distinguished. The first is used for locking and unlocking the SAM.

The second kind is used to get the access rights to execute certain commands. It only affects the SAM status for the LC it is executed over and can be used to set up a SAC over this LC if preferred by the host. Once authenticated, three different protection modes on the LC are foreseen: plain, MAC Protection and Full Protection (i.e. by MACs and encryption). This host authentication is executed by using the SAM_AuthenticateHost command.

Note that whether and when host authentications (be it for unlocking or for gaining access rights) are required depends on the SAM configuration and is explained in Ref. 1.

8.6 MIFARE SAM AV2 command set

For better readability of the following command descriptions, the logical channel number of the CLA byte is set to default 00b.

8.6.1 SAM security and configuration commands

Table 7. SAM security and configuration commands

Command	Description
SAM_DisableCrypto	This command allows the permanent and irreversible disabling of the cryptographic functionality of the MIFARE SAM AV2. Successful host authentication with one of the three keys stored in KeyNo 00h is required to send this command.
SAM_LockUnlock	The command SAM_LockUnlock (INS = 10h) is used to run a mutual authentication between the SAM and host system. The host authentication consists of three parts. Such an authentication proves that both the SAM and the host contain the same secret, namely the AES key Kx. The terminology, notations and state descriptions for SAM_LockUnlock are provided in Ref. 1.
SAM_AuthenticateHost	**AV1 compatibility mode**: The command SAM_AuthenticateHost is used to run a mutual 3-pass authentication between the MIFARE SAM AV2 and host system. Such an authentication proves that both the MIFARE SAM AV2 and the host contain the same secret, namely a DES, TDEA or AES key and generates a session key for further cryptographic operations. A host authentication is required to: • Load or update keys into the MIFARE SAM AV2 • Modify key usage counter limits • Activate the MIFARE SAM AV2 after reset (if configured accordingly in the configuration settings (SET) of KeyNo 00h)
SAM_ActivateOfflineKey	SAM_ActivateOfflineKey is to be used in AV2 mode to activate both OfflineCrypto and OfflineChange keys.
SAM_LoadInitVector	The command SAM_LoadInitVector is used to load an init vector for the next cryptographic operation into the MIFARE SAM AV2. The loaded init vector will be applied in the next cryptographic operation independent from the 'Keep IV' setting of the key entry except for the authentication commands where the init vector is reset to zero.
SAM_KillAuthentication	**AV1 compatibility mode:** Invalidates any kind of authentication in the logical channel the command is issued.
SAM_SelectApplication	The command SAM_SelectApplication is the equivalent of the SelectApplication command of DESFire. The MIFARE SAM AV2 generates a list of available keys linked to the specified Application ID as defined in the key entry property 'DF_AID'. The MIFARE SAM AV2 generates a list of available keys per DESFire AID and DESFire key number. For every key number, up to 6 key versions can be stored in the list (so it can read the keys from maximum two key entries per DESFire AID and DESFire key number). This list is filled starting with key entry zero. If the KST contains more than 6 key versions per DESFire AID and DESFIRE key number, only the first 6 versions will be listed.

Table 7. SAM security and configuration commands *…continued*

Command	Description
SAM_IsoGetChallenge/ SAM_GetRandom	**AV1 compatibility mode** In AV1 compatibility mode, this is the first part of an ISO compliant authentication sequence returning a random number. The command can obviously also be used for simply generating a random number but it has to be taken into account that the MIFARE SAM AV2 internally is set into a state indicating that an authentication procedure is ongoing, if the requested random number length is 8 byte or 16 byte. Consequently, the command called after getting the random number will be aborted (except SAM_IsoExternalAuthenticate). After this abortion the MIFARE SAM AV2 resets its state and returns to normal operation. For a complete and valid authentication procedure, the three commands SAM_IsoGetChallenge, SAM_IsoExternalAuthenticate and SAM_IsoInternalAuthenticate have to be called in sequence without interrupting the sequence by another command. **AV2 mode** In AV2 mode, this command is only available to get random numbers. In this case, there are no special constraints on the expected length for the challenge.
SAM_IsoExternalAuthenticate	This command is part of an ISO compliant authentication procedure consisting of SAM_IsoGetChallenge, SAM_IsoExternalAuthenticate and SAM_IsoInternalAuthenticate. It can be used by a host for authenticating the MIFARE SAM AV2. Note that this command is only available in AV1 compatibility mode. Such an authentication proves that both the MIFARE SAM AV2 and the host contain the same secret, namely a DES, TDEA or AES key, and generates a session key for further cryptographic operations.
SAM_IsoInternalAuthenticate	This command is part of an ISO compliant authentication procedure consisting of SAM_IsoGetChallenge, SAM_IsoExternalAuthenticate and SAM_IsoInternalAuthenticate. It can be used by a host for authenticating the MIFARE SAM AV2. Note that this command is only available in AV1 compatibility mode. Such an authentication proves that both the MIFARE SAM AV2 and the host contain the same secret, namely a DES, TDEA or AES key, and generates a session key for further cryptographic operations.
SAM_GetVersion	The SAM_GetVersion command returns manufacturing related data of the MIFARE SAM AV2. The SAM_GetVersion command can be used to detect whether a SAM has been switched to the MIFARE SAM AV2 mode.
SAM_Sleep	Will force the MIFARE SAM AV2 to put a connected RC52x or RC663 into sleep mode and itself into idle mode to reduce power consumption. The MIFARE SAM AV2 will answer the command and afterwards switch to idle mode. The MIFARE SAM AV2 will automatically return to normal operation after receiving the first character of the next command. The RC52x or RC663 will stay in sleep mode until a command is issued which utilizes the reader IC. Then the MIFARE SAM AV2 automatically carries out the wake-up sequence before starting the requested operation.

8.6.2 SAM key management commands

Table 8. SAM key management commands

Command	Description
AV1 compatibility mode	
SAM_ChangeKeyEntry	This command updates any key entry of the KST. The complete data set of the full key entry must always be sent, and it will be programmed to the non-volatile memory of the MIFARE SAM AV2 as defined in the non-volatile ProMas.
SAM_GetKeyEntry	The SAM_GetKeyEntry command allows reading the contents of the key entry specified in the parameter KeyNo. Instead of the full keys on positions a, b and c, only their key version will be returned, each packed in one byte. This command can be issued without valid (host) authentication.
SAM_ChangeKUCEntry	This command updates any key usage counter entry stored in the MIFARE SAM AV2. Always limit, KeyNoCKUC and KeyVCKUC have to be sent; the parameter ProMas defines which properties are programmed into the MIFARE SAM AV2 non-volatile memory. Successful host authentication with the key specified in KeyNoCKUC of the current KUC entry is required.
SAM_GetKUCEntry	The SAM_GetKUCEntry command allows reading the data of the key usage counter entry specified within the Parameter RefNoKUC. This command can be issued without valid (host) authentication.
SAM_DumpSessionKey	The command SAM_DumpSessionKey can be used to retrieve the session key generated by the MIFARE SAM AV2. The session key could be retrieved either in plain or encrypted with the session key of any logical channel. A CRC is appended before encryption as usual. This feature is necessary if cryptographic operations like en-/decipher should be handled by the terminal microcontroller instead of the MIFARE SAM AV2. As this feature can be seen as a potential security risk if not used in the correct way, it can be en-/disabled using the configuration settings of every key entry.
SAM_DisableKeyEntry	The SAM_DisableKeyEntry command disables a key entry. After executing this command, the corresponding disable flag in the key entry is set and the key entry cannot be used anymore for authentication and key change procedures. The key entry can still be read by a SAM_GetKeyEntry command. To reactivate the entry, a SAM_ChangeKeyEntry command has to be issued. All fields in the key entry can still be changed by this command even if the entry has been disabled.
AV2 Mode The following rows give an outlook of the changes compared to the AV1 compatibility mode. All commands except SAM_GetKUCEntry got partially or completely redefined for the AV2 mode. For more information see Ref. 1.	
SAM_ChangeKeyEntry and SAM_ChangeKUCEntry	In the AV1 version, there are two possibilities for changing key and KUC entries via the SAM_ChangeKeyEntry and SAM_ChangeKUCEntry respectively. Which possibility is used, depends on whether the "allow crypto with secret key" of the change key, i.e. the key referenced by KeyNoCEK or KeyNoCKUC respectively, was set. If set, this allowed for offline preparation of the key/KUC changing cryptogram. In the new MIFARE SAM AV2 mode, these two possibilities are still supported, but which possibility is used depends on the key class of the change key. Change keys are either Host Keys or OfflineChange Keys. The second class will allow offline command generation.
SAM_GetKeyEntry	The SAM_GetKeyEntry command allows reading the contents of the key entry specified in the parameter KeyNo. Instead of the full keys on positions a, b and c, only their key version will be returned, each packed in one byte. This command can be issued without valid (host) authentication.

Table 8. SAM key management commands *...continued*

Command	Description
SAM_DumpSessionKey	The command SAM_DumpSessionKey can only be used to retrieve the session key of an established authentication with a DESFire or MIFARE Plus PICC. So an active PICC authentication (for these card types) is required. The session key can be retrieved in plain or encrypted, depending on the SAM-Host protection mode of the logical channel. In Plain and MAC Protection mode, the dump is done in plain; in Full Protection the key is encrypted (as any other response data field). Under MAC Protection, the response data field can optionally be encrypted if requested via setting bit 0 of P1. This command cannot be used for secret key dumping.
SAM_DumpSecretKey	SAM_DumpSecretKey allows dumping any of the PICC keys (except MIFARE Classic keys) or OfflineCrypto keys.
SAM_DisableKeyEntry	In AV2 mode, two possibilities are supported, similar to the SAM_ChangeKeyEntry command. Which possibility is used depends on the key class of the change key. Change keys are either Host Keys or OfflineChange Keys. The second class will allow offline command generation.

8.6.3 Data processing commands

Table 9. Data processing commands

Command	Description
AV1 compatibility mode	
SAM_Verify_MAC	The SAM_Verify_MAC command verifies the MAC which was sent by the DESFire PICC or any other system based on the given MACed plain text data and the currently valid cryptographic key. The applied MAC algorithm depends on the key typ. The command can also be used for verifying only a part of a MAC. The number of MAC bytes to be verified is defined by parameter P2.
SAM_Generate_MAC	The SAM_Generate_MAC command creates a MAC which is meant to be sent to the DESFire PICC or any other system based on the given plain text data and the currently valid cryptographic key. The applied MAC algorithm depends on the key type.
SAM_Decipher_Data	The SAM_Decipher_Data command deciphers data packages sent by a DESFire PICC, any other system or a MIFARE card based on the currently valid cryptographic key and returns plain data to the PCD.
SAM_Encipher_Data	The SAM_Encipher_Data command creates data packages which are meant to be sent to a DESFire PICC or any other system based on the given plain text data and the currently valid cryptographic key. To do so, the plain data is en-ciphered in cipher block chaining send mode. CRC and padding bytes are appended automatically.

AV2 Mode

The MIFARE SAM AV1 supported the execution of cryptographic operations (MACing, encryption) using the SAM data processing commands with a key that allowed "Crypto with secret key". So the same primitives as used for the DESFire communication are also accessible for so-called offline cryptographic operations (i.e. crypto operations that are not part of the SAM-Host or SAM-PICC communication protocols).

For the MIFARE SAM AV2 this kind of functionality is still supported. The "Crypto with secret key" operation is replaced by a separate key class, called OfflineCrypto Keys. The existing SAM data processing commands are extended to support full length MAC generation and verification; also new commands for executing standard CBC encryption and decryption are provided.

The existing SAM data processing commands (SAM_Generate_MAC, SAM_Verify_MAC, SAM_Encipher_Data and SAM_Decipher_Data) can still be used to support DESFire communication, by issuing them in an LC with an active PICC authentication (SAM_AuthenticatePICC). These commands and the new SAM_EncipherOffline_Data and SAM_DecipherOffline_Data can be used with OfflineCrypto Keys if issued in an LC with an active OfflineCrypto key.

Table 9. Data processing commands *…continued*

Command	Description
SAM_Verify_MAC	The SAM_Verify_MAC command verifies the MAC which was sent by the DESFire PICC or any other system based on the given MACed plain text data and the currently valid cryptographic key. The valid key has been activated using a valid PICC authentication (SAM_AuthenticatePICC, SAM_ISOAuthenticatePICC) in case of a PICC Key or using a valid key activation (SAM_ActivateOfflineKey) in case of an OfflineCrypto Key. The applied MAC algorithm depends on the key type. In case of the AES key types and the (3)DES key types 3 and 6, the standard CMAC algorithm is applied.
SAM_Generate_MAC	The SAM_Generate_MAC command creates a MAC which is meant to be sent to the DESFire PICC or any other system based on the given plain text data and the currently valid cryptographic key. The valid key has been activated using a valid PICC authentication (SAM_AuthenticatePICC, SAM_ISOAuthenticatePICC) in case of a PICC Key or using a valid key activation (SAM_ActivateOfflineKey) in case of an OfflineCrypto Key. The applied MAC algorithm depends on the key type. In case of the AES key types and the (3)DES key types 3 and 6, the standard CMAC algorithm is applied.
SAM_Decipher_Data	Same operation as in MIFARE SAM AV1 compatibility mode performed with either a valid PICC authentication (SAM_AuthenticatePICC, SAM_ISOAuthenticatePICC or SAM_AuthenticateMIFARE) in case of a PICC Key or a valid key activation (SAM_ActivateOfflineKey) in case of an OfflineCrypto Key.
SAM_Encipher_Data	Same operation as in AV1 compatibility mode and same description.
SAM_DecipherOffline_Data	The new SAM_DecipherOffline_Data command decrypts data received from any other system based on the given cipher text data and the currently valid cryptographic OfflineCrypto Key. The valid key has been activated using a valid key activation (SAM_ActivateOfflineKey). The applied decryption is the block cipher algorithm depending on the key type in CBC mode. The IV needs to be loaded via the SAM_LoadInitVector command before issuing this command. If no IV was loaded, the zero byte IV is applied. No padding is removed from the decrypted plain text, so the output length equals the input length. The total input size must be a multiple of the block size of the underlying block cipher (depending on the key type). In case of command chaining, the SAM immediately starts returning decrypted data for the received blocks.
	The new SAM_EncipherOffline_Data command encrypts data received from any other system based on the given cipher text data and the currently valid cryptographic OfflineCrypto Key. The valid key has been activated using a valid key activation (SAM_ActivateOfflineKey). The applied decryption is the block cipher algorithm depending on the key type in CBC mode. The IV needs to be loaded via the SAM_LoadInitVector command before issuing this command. If no IV was loaded, the zero byte IV is applied. No padding is added to the plain text, so the output length equals the input length. As a consequence, the total input size must be a multiple of the block size of the underlying block cipher (depending on the key type). In case of command chaining, the SAM immediately starts returning encrypted data for the received blocks.

8.6.4 Public Key Infrastructure (PKI) commands

PKI commands are available to generate public key pairs, to import public keys or key pairs, to export public keys or key pairs, to generate and to validate signatures, to compute hashes suitable for signature operations and to manage the symmetric Key Storage Table.

PKI commands are only available in AV2 mode.

Table 10. Public Key Infrastructure (PKI) commands

Command	Description
PKI_GenerateKeyPair	The PKI command PKI_GenerateKeyPair creates a pair of a public and a private key. MIFARE SAM AV2 only supports the CRT format. A successful host authentication in the LC using SAM_AuthenticateHost with a Host Key is required to execute the PKI_GenerateKeyPair command.
PKI_ImportKey	The PKI command PKI_ImportKey imports an RSA key. This can be either a public key or a full key pair (including a private key). When a change key (see Ref. 1) is specified, a successful host authentication in the LC using SAM_AuthenticateHost with a Host Key is required to execute the PKI_ImportKey command.
PKI_ExportPrivateKey	The PKI command PKI_ExportPrivateKey exports a full RSA key entry (i.e including the private key if present). The key pair is exported in CRT format. This command is intended for private key backup after having it created with MIFARE SAM AV2. For this reason, this command will only be accepted if the key entry includes a private key and private key export is allowed by the PKI SET configuration of the addressed key. The command is part of the restricted command set and requires protection with a Host Key change key.
PKI_ExportPublicKey	The PKI command PKI_ExportPublicKey exports the public key part of a RSA key pair. The command is part of the general command set, so its protection depends on the general SAM-Host communication protection.
PKI_UpdateKeyEntries	The PKI_UpdateKeyEntries command can be used to change key entries of the symmetric key storage (KST). Executing this command does not require any protection coming from the change key of the key entries (e.g. a Host Authentication in case of a Host Key). Instead the command's execution is protected by asymmetric techniques using the PKI support of the SAM. The command is protected by encrypting the key entries using the RSA encryption. On top a digital signature is added using the RSA signature algorithm. This allows offline preparation of the cryptogram. The same hashing algorithm is to be used for both MGFs and for the digital signature handling (as indicated by the P1 byte).
PKI_GenerateHash	The PKI command PKI_GererateHash computes the hash on a data string. The algorithm to be used to compute the hash is selected through P1.
PKI_GenerateSignature	The PKI command PKI_GenerateSignature generates a signature on a hash given as input using one of the two private keys stored in the PKI Key Storage Table.
PKI_SendSignature	The PKI command PKI_SendSignature returns a pre-computed signature. The returned signature is protected according to the SAM-Host protection in place on the corresponding logical channel.
PKI_VerifySignature	The PKI command PKI_VerifySignature verifies the correctness of a signature.

8.6.5 MIFARE Plus in non-X-mode commands

This section describes the SAM commands that can be used to prepare MIFARE Plus commands. The SAM maintains the MIFARE Plus state (e.g. the read and write counters).

Table 11. MIFARE Plus in non-X mode commands

Command	Description
SAM_AuthenticateMFP	SAM_AuthenticateMFP can be used for all MIFARE Plus authentications (e.g. SL1, SL2, SL3, originality keys, SL2 re-authentication). The choice of whether a first or following authentication is to be performed is indicated in the parameters of the command. Also the user has to indicate which session key derivation needs to be used afterwards: no session keys needed (SL1 card authentication, originality keys authentication), key derivation to continue with SAM_AuthenticateMIFARE (SL2) or session key derivation to continue with normal MIFARE Plus transaction (SL3). SAM_AuthenticateMFP only supports the 2-part version of the MIFARE Plus Authentication.
SAM_CombinedReadMFP	SAM_CombinedReadMFP handles either a MIFARE Plus Read command, a MIFARE Plus Read Response or both.
SAM_CombinedWriteMFP	SAM_CombinedWriteMFP handles either a MIFARE Plus write command (Write, Increment, Decrement, Transfer, Restore, Increment Transfer or Decrement Transfer) or a MIFARE Plus write response. Bit 0 of P1 indicates whether it is a command or a response.
SAM_ChangeKeyMFP	SAM_ChangeKeyMFP computes the command required to replace a MIFARE Plus key with one of the keys stored in the SAM.
SAM_VirtualCardSupportMFP	SAM_VirtualCardSupportMFP handles the MIFARE Plus VCS and VCSL commands. One SAM_VirtualCardSupport can handle up to 5 command sets. A command set covers a block of VCS commands and one concluding VCSL command.
SAM_SelectVirtualCardMFP	SAM_SelectVirtualCardMFP handles the MIFARE Plus SVC command.
SAM_ProximityCheckMFP	SAM_ProximityCheckMFP is performed in two steps. In the first step, given the data collected during the execution of the proximity check protocol with the MIFARE Plus PICC, the SAM computes the MAC needed for the final proximity check command. In the second step, the SAM verifies the MAC received from the MIFARE Plus PICC.

8.6.6 MIFARE Classic in non-X-mode commands

The commands in this section can both be used to execute a transaction with a MIFARE Classic card and with a MIFARE Plus card in SL2. In the second case, SAM_AuthenticateMIFARE is to be used after SAM_AuthenticateMFP to complete a MFP SL2 authentication.

In both cases, after the authentication, the other SAM_xxxMIFARE commands and the data processing commands SAM_Decipher_Data and SAM_Encipher_Data can be used for further processing.

Table 12. MIFARE Classic in non-X-mode commands

Command	Description
SAM_Authenticate MIFARE	n this procedure, both the MIFARE card as well as the MIFARE SAM AV2 device show in an encrypted way that they posses the same secret which especially means the same key.
SAM_ChangeKey MIFARE	AV1 compatibility mode This command is intended to change a key in a MIFARE card. The command offers the possibility to prepare an encrypted stream to be written to a MIFARE 1k or MIFARE 4k card containing the desired keys and the given access conditions on the one hand and reading out a single MIFARE key to be used for any kind of MIFARE transaction in a host system directly on the other hand. In the latter case, the key can be retrieved encrypted from the MIFARE SAM AV2 using the current available session key of the channel (host authentication required). The first case requires an active MIFARE authentication for producing the stream to be sent to the card.AV2 mode (used for key retrieval) In MIFARE SAM AV2 mode, the existing command, SAM_ChangeKeyMIFARE (used for key retrieval), can still be used to retrieve a PICC Key of key type 010, i.e. a MIFARE Classic key. The use of this command to change keys on MIFARE Classic cards is the same as the one described for the AV1 compatibility mode. The only difference with AV1 is that whether the secret key is retrieved in plain or encrypted depends on the SAM-Host protection mode of the logical channel.

8.6.7 DESFire and ULC in non-X-mode commands

Table 13. DESFire and ULC in non-X-mode commands

Command	Description
SAM_AuthenticatePICC	In this procedure both the PICC as well as the MIFARE SAM AV2 device show in an encrypted way that they posses the same secret which especially means the same key. This procedure not only confirms that both entities are permitted to do operations on each other but also creates a session key which can be used to keep the further communication path secure. As the name ‘session key’ implicitly indicates, each time a new authentication procedure is successfully completed a new key for further cryptographic operations is obtained.
SAM_IsoAuthenticatePICC	The ISO authentication procedure is intended to authenticate with a card using the standard ISO commands GetChallenge, ExternalAuthenticate and InternalAuthenticate. This authentication procedure can be used to authenticate a DESFire PICC but also another MIFARE SAM AV2. However, the MIFARE SAM AV2 will treat the authentication procedure as a PICC authentication, which means that commands requiring a host authentication will not be available.
SAM_ChangeKeyPICC	This command generates the cryptogram that has to be sent to the PICC in order to change any key stored in the PICC. Both the current and the new key need to be stored in the KST to execute this command. This means a new PICC key needs to be loaded into the MIFARE SAM AV2, prior to issuing this command.

8.6.8 RC52x or RC663 configuration commands

Table 14. RC522x or RC663 configuration commands

Command	Description
RC_ReadRegister	Read the content of one or more register(s) of the connected reader chip. The command allows reading 255 registers with one command. If a register address is listed more than once in the data field, the content of this register will be re-read every time.
RC_WriteRegister	Write the content of one or more register(s) of the connected reader chip. The command allows writing 127 registers with one command. If a register address with its related content is listed more than once in the data field, the content of this register will be re-written every time.
RC_RFControl	This command allows the radio frequency field to be turned off and on. The basic behavior is the reset functionality where the controller turns off the field for the time given in the data field. If a zero value is passed, the field is totally turned off. After turning off the field, to turn it on again, the command can be issued with any value other than zero. Take into account that the passed time value also in this case will force the MIFARE SAM AV2 to wait this additional time until turning on the field again.
RC_Init	Establishes the serial connection between MIFARE SAM AV2 and RC52x or RC663 and initializes the reader chip with the register values stored in the selected register value set.
RC_LoadRegister ValueSet	Stores a customer defined register value set for the RC52x or RC663 in the non-volatile memory of the MIFARE SAM AV2. This set can then be used for initializing the reader chip with the RC_Init command. The address of and the related value for the register have to be placed consecutively in the command data field of the APDU.

8.6.9 ISO14443 commands

Table 15. ISO14443 commands

Command	Description
ISO14443-3_Request_Wakeup	Issue a request or wake-up command.
ISO14443-3_Anticollision_Select	Perform bit-wise anticollision and select. The anticollision and the following select are performed according to the select code in the data field.
ISO14443-3_ActivateIdle	Carries out one or several request - anticollision - select sequences and returns the SAK and the UID of the selected card(s). The ATQA is returned for every request issued, this means for every newly activated card. Due to the fact that the resulting ATQA is the OR-function of all ATQAs, the value may change frequently.
ISO14443-3_ActivateWakeup	The command reactivates and selects a card that has previously been set to Halt state. The command takes the UID of the card to reactivate.
ISO14443-3_HaltA	The command puts a selected card into Halt state.
ISO14443-3_TransparentExchange	Exchange bytes/bits transparently. The MIFARE SAM AV2 will take the user data and send it without changing, inserting or appending any content to the contactless card. Appending of a CRC, time-out settings, etc. have to be configured by directly writing the RC52x or RC663 registers. Take into account that switching settings of the reader chip influence all subsequent MIFARE SAM AV2 commands proposing the correct reader chip settings, i.e. ISO14443- 4_Exchange.
ISO14443-4_RATS_PPS	Execute a combined RATS and PPS sequence to prepare a card for T=CL data exchange. The CID assigned to the card will be assigned to the current logical channel. This means, every further ISO14443-4 command issued in this logical channel will be executed using this CID automatically.
ISO14443-4_Init	Initialize the T = CL protocol. The intent of this command is to configure the protocol for data exchanges. This is necessary if a card was already activated and configured for doing data exchanges without using the ISO14443-4_RATS_PPS command.
ISO14443-4_Exchange	Exchange bytes according to ISO/IEC 14443-4 T = CL protocol.

Table 15. ISO14443 commands *…continued*

Command	Description
ISO14443-4_PresenceCheck	Check if an activated card is still in the field.
ISO14443-4_Deselect	Deselect an activated card. The CID is freed by this command. If the deselect fails, the CID will not be freed and cannot be used for activating another card. This behavior might be overridden by setting a flag in the P1 byte. CIDs can also be freed using the ISO14443-4_FreeCID command.
ISO14443-4_FreeCID	Free one, more, or all currently assigned CIDs. This command might be necessary if several deselect commands failed and the CIDs were not forced to be freed but the card is deactivated or no longer available in the field.

8.6.10 MIFARE Classic in X-mode commands

The commands in this section can both be used to execute a transaction with a MIFARE Classic card and with a MIFARE Plus card in SL2. In the second case, MF_Authenticate, MF_AuthenticatedRead or MF_AuthenticatedWrite is to be used after MFP_Authenticate to complete a MFP SL2 authentication. Afterwards, the other MF_xxx commands can be used for further processing.

Table 16. MIFARE Classic in X-mode commands

Command	Description
MF_Authenticate	Performs an authentication with a MIFARE card. The MIFARE key has to be stored in the MIFARE SAM AV2 and is referenced by a parameter in the command data field. The key can be diversified if necessary.
MF_Read	Read one or several blocks of a MIFARE card and return the data. If more than one block is read, the MIFARE SAM AV2 accesses the blocks in the same order as addresses listed in the command data field. The order of the returned data is the same as the order of addresses in the data field.
MF_Write	Write one or several blocks of a MIFARE card. If more than one block is written, the MIFARE SAM AV2 accesses the blocks in the same order as addresses listed in the command data field. The command supports writing of 16 bytes encrypted for MIFARE 1k and MIFARE 4k cards as well as writing 16 bytes or 4 bytes plain for MIFARE Ultralight cards. The length can be selected by bit 0 of parameter byte P2. If 16 bytes block write is selected, the MIFARE SAM AV2 decides whether encryption shall be used by checking the authentication state. If a MIFARE authentication has been completed, the data is encrypted. Encrypted writing of 4 byte blocks is not supported.
MF_ValueWrite	Write one or several value blocks of a MIFARE card. If more than one block is written, the MIFARE SAM AV2 accesses the blocks in the same order as addresses listed in the command data field. Since a MIFARE card uses 12 bytes for storing a four-byte value, the address to write in the last four bytes has to be specified by the user (’address’ parameter).
MF_Increment	Increment one or several value blocks on a MIFARE card. Every increment is confirmed automatically by sending the transfer command directly afterwards. The user has to define the source address of the value block to be incremented and the destination address of the value block to store the result. If more than one block is incremented, the MIFARE SAM AV2 accesses the blocks in the same order as addresses listed in the command data field.
MF_Decrement	Decrement one or several value blocks on a MIFARE card. Every decrement is confirmed automatically by sending the Transfer command directly afterwards. The user has to define the source address of the value block to be decremented and the destination address of the value block to store the result. If more than one block is decremented, the MIFARE SAM AV2 accesses the blocks in the same order as addresses listed in the command data field.
MF_Restore	Copy one or several value blocks on a MIFARE card. If more than one block is copied, the MIFARE SAM AV2 accesses the blocks in the same order as addresses listed in the command data field. The order of the status code is the same as the order of addresses in the data field.

Table 16. MIFARE Classic in X-mode commands *…continued*

Command	Description
MF_Authenticated Read	Performs an authentication with subsequent reading of blocks on a MIFARE card. The command allows authenticating and reading several different blocks on the card within one command. Several blocks can be read without re-authenticating, but also several blocks with different authentications. For each block address needing a new authentication, the key to authenticate with and whether it shall be diversified has to be specified. If a key is used for accessing different blocks but a new authentication is necessary, these blocks have to be listed consecutively in the data field and the re-use to be indicated by a flag. If more than one block is read, the MIFARE SAM AV2 accesses the blocks in the same order as addresses listed in the command data field. The order of the returned data is the same as the order of addresses in the data field.
MF_Authenticated Write	Performs an authentication with subsequent writing of blocks on a MIFARE card. The command allows authenticating and writing several different blocks on the card within one command. Several blocks can be written without re-authenticating, but also several blocks with different authentications. For each block address needing a new authentication, the key to authenticate with and whether it shall be diversified has to be specified. If a key is used for accessing different blocks, these blocks have to be listed consecutively in the data field and the re-use to be indicated by a flag. If more than one block is written, the MIFARE SAM AV2 accesses the blocks in the same order as addresses listed in the command data field.
MF_ChangeKey	This command is intended to change a key in a MIFARE card. The command offers the possibility to prepare and write an encrypted data stream to a MIFARE 1k or MIFARE 4k card containing the desired keys and the given access conditions. The first case requires an active MIFARE authentication for producing the stream to be sent to the card. This command is able to generate a diversified MIFARE standard key, based on a MIFARE key stored in the MIFARE SAM AV2, a TDEA key stored in the MIFARE SAM AV2, the UID of the MIFARE standard PICC and the block address on the MIFARE standard card. The TDEA key applied for the diversification is referenced in the MIFARE key entry.

8.6.11 MIFARE Plus in X-mode commands

This chapter describes the commands for the MIFARE Plus PICC's when the MIFARE SAM AV2 is used in MIFARE SAM AV2 mode.

When a MIFARE Plus communication is established between the SAM and a MIFARE Plus PICC, the corresponding SAM logical channel maintains the state (e.g. the read and write counters) required to manage the secure messaging with the MIFARE Plus PICC.

Table 17. MIFARE Plus in X-mode commands

Command	Description
MFP_WritePerso	MFP_WritePerso is a multi-block write command. It performs up to 13 MFP WritePerso commands. If more than 13 values are to be updated, several MFP_WritePerso are to be issued. There is no command chaining for this command.
MFP_Authenticate	MFP_Authenticate performs all MIFARE Plus authentications (e.g. SL1, SL2, SL3, originality keys...). The choice of whether a first or following authentication is to be performed is indicated in the parameters of the command. Also the user has to indicate which session key derivation needs to be used afterwards: no session keys needed (SL1 card authentication, originality keys authentication), key derivation to continue with MF_Authenticate (SL2) or session key derivation to continue with normal MIFARE Plus transaction (SL3).
MFP_CombinedRead	MFP_CombinedRead performs one MIFARE Plus read command.
MFP_CombinedWrite	MFP_CombinedWrite performs a MIFARE Plus write command where a write command can be a MIFARE Plus Write, Increment, Decrement, Transfer, Restore, Increment Transfer or Decrement Transfer command. Each MFP_CombinedWrite command is restricted to one MIFARE Plus write command.
MFP_ChangeKey	MFP_ChangeKey replaces one of the MIFARE Plus PICC keys by one of the keys stored in the SAM.
MFP_ProximityCheck	MFP_ProximityCheck performs the complete MIFARE Plus proximity check between MIFARE SAM AV2 and the MIFARE Plus PICC. It performs the PPC, the one or more PC's and the VPC command. As this is the X-mode command, the proximity time measurement is handled by a MFRC52X reader IC time-out. The reader IC will use the ISO14443-3 minimal frame delay time, as a time-out value for the PICC response to the MIFARE Plus Proximity Check command(s) sent. In case the proximity check is executed with an MFP authentication, the MAC session key of this authentication will be used for the MIFARE Plus Verify Proximity Check (VPC). The command also foresees random VPC processing as recommended in some cases for privacy reasons.
MFP_VirtualCardSupport	MFP_VirtualCardSupport sends as many MIFARE Plus VCS and VCSL commands to the MIFARE Plus PICC as specified in the command. MFP_VirtualCardSupport accepts up to 5 command sets. MFP_VirtualCardSupport returns the MIFARE Plus PICC responses to the corresponding VCSL commands. A command set is made of commands. For each command the key duo is specified (i.e. the SAM key to be used for MAC and the SAM key to be used for ENC) together with the VCIID to be advertised by the SAM to the MIFARE Plus PICC. Given a command set, sizeof(command set)-1 VCS commands are sent with one concluding VCSL command.
MFP_SelectVirtualCard	MFP_SelectVirtualCard sends a MIFARE Plus SVC command to the MIFARE Plus PICC. If no successful entry for this IID can be found (from MFP_VirtualCardSupport processing), the SAM will still send an SVC command (with random MAC) to the card. On successful execution (both valid and invalid IID), the internal VC table is invalidated. Note that MIFARE SAM AV2 does not support multiple VC selection protocols to be executed in parallel. The user needs to ensure the VC selection is completed before starting another on any of the LCs, as starting VC selection with SAM_VirtualCardSupportMFP or MFP_VirtualCardSupport will also invalidate the existing internal VC table (if any).

8.6.12 DESFire and ULC in X-mode commands

Table 18. DESFire and ULC in X-mode commands

Command	Description
DESFire_AuthenticatePICC	In this procedure both the PICC as well as the MIFARE SAM AV2 device, show in an encrypted way that they posses the same secret which especially means the same key. This procedure not only confirms that both entities are permitted to do operations on each other but also creates a session key which can be used to keep the communication path secure. As the name ‘session key’ implicitly indicates, each time a new authentication procedure is successfully completed a new key for further cryptographic operations is obtained.
DESFire_ChangeKeyPICC	This command generates the cryptogram that has to be sent to the PICC in order to change any key stored in the PICC. Both the current and the new key need to be stored in the KST to execute this command. This means a new PICC key needs to be loaded into the MIFARE SAM AV2, prior to issuing this command.
DESFire_WriteX	Write data encrypted or MACed on a DESFire PICC. This command shall be used to issue the ChangeKeySettings, WriteData, Credit, Debit, LimitedCredit or WriteRecord command. It takes the data to be sent to the DESFire and applies the encryption or MACing mechanism starting from an indicated index. The user is responsible for providing the correct command frame including the command code, the parameter bytes and the plain data as specified for the DESFire PICC. The indication from which position on the crypto mechanism shall be applied will normally be the first data byte of the command frame. The MIFARE SAM AV2 will automatically adapt the amount of bytes to send to the PICC after encryption of data or adding the MAC, respectively.
DESFire_ReadX	Read encrypted or MACed data from the DESFire PICC. This command shall be used to issue the ReadData, GetValue, or ReadRecords command. It takes the data to be sent to the DESFire and applies the decryption and MAC verification mechanism to the received data. Afterwards the MIFARE SAM AV2 returns the decrypted or verified plain data. The user is responsible for providing the correct command frame including the command code and the parameter bytes as specified for the DESFire PICC. This command frame will be sent directly to the DESFire. This is also the case for commands applying application chaining.
ULC_ AuthenticatePICC	The ULC_AuthenticatePICC command is needed to authenticate to a MIFARE Ultralight C card.

9. Limiting values

Table 19. Limiting values [1]

In accordance with the Absolute Maximum Rating System (IEC 60134). Voltages are referenced to VSS (ground = 0 V).

Symbol	Parameter	Conditions		Min	Max	Unit
V_{DD}	supply voltage			−0.5	+6.0	V
V_I	input voltage	on any signal pad		−0.5	V_{DD} +0.5	V
I_I	input current	on pads IO1, IO2 or IO3		-	±15.0	mA
I_O	output current					
I_{lu}	latch-up current	$V_I < 0$ or $V_I > V_{DD}$		-	±100	mA
V_{ESD}	electrostatic discharge voltage	on pads VDD, VSS, CLK, RST, IO1, IO2, IO3	[2]	-	±4.0	kV
		on pads LA, LB	[2]	-	±2.0	kV
P_{tot}(pack)	total power dissipation per package		[3]	-	1	W

[1] Stresses beyond those listed may cause permanent damage to the device. These are stress ratings only and functional operation of the device at these or any other conditions beyond those indicated under “recommended operating conditions” is not implied. Exposure to absolute-maximum-rated conditions for extended periods may affect device reliability.

[2] MIL Standard 883-D method 3015; Human body model; C = 100 pF, R = 1.5 kΩ; T_{amb} = −25 °C to +85 °C.

[3] Depending on appropriate thermal resistance of the package.

10. Characteristics

Table 20. Recommended operating conditions

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
V_{DD}	supply voltage	5 V operation	4.5	5.0	5.5	V
		3 V operation	2.7	3.0	3.3	V
V_I	input voltage	on digital inputs and digital I/O pads	0	-	V_{DD}	V
T_{amb}	ambient temperature		−25	-	+85	°C

Table 21. Electrical characteristics of IC supply voltage

V_{DD}; V_{SS} = 0 V; T_{amb} = −25 °C to +85 °C

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
V_{DD}	supply voltage	Class A: 5 V range	4.5	5.0	5.5	V
		Class B: 3 V range	2.7	3.0	3.3	V

11. Abbreviations

Table 22. Abbreviations

Acronym	Description
2TDEA	2 Key TDEA
3TDEA	3 Key TDEA
AES	Advanced Encryption Standard
AID	Application IDentifier
APDU	Application Protocol Data Unit
AppData	Application Data
ATQA	Answer To reQuest (Type A)
ATR	Answer To Reset
ATS	Answer To Select
Auth mode	Authentication Mode
Authent	Authentication
CBC	Cipher Block Chaining (a block cipher mode)
CID	Card IDentifier
CLA	CLAss
CMAC	Ciphered-based MAC
CmdCode	Command Code
CmdSettings	Command Settings
CRC	Cyclic Redundancy Check
CRC16	16 bit CRC
CRC32	32 bit CRC
CRT	Chinese Remainder Theorem
CurVal	Current Value of key usage counter
CWT	Character Waiting Time
DES	Data Encryption Standard
DF_AID	DESFire AID
DF_KeyNo	DESFire Key Number
DFKeyNo	DESFire Key Number
Div	Diversification
DivInp	Diversification Input
DRI	Divisor Receive Integer
DSI	Divisor Send Integer
EEPROM	Electrically Erasable Programmable Read Only Memory
ek(x)	Encrypted 'x'
ekNo(x)	Encrypted Number 'x'
FIFO	First In First Out
FIPS	Federal Information Processing Standard
FSC	Frame Size for Card
FSCI	Frame Size for Card Integer
FSD	Frame Size for Device

Table 22. Abbreviations *...continued*

Acronym	Description
FSDI	Frame Size for Device Integer
FWI	Frame Waiting time Integer
INS	INStruction code
ISO	International Organization for Standardization
IV	Initial Vector (input parameter to some block cipher modes)
KeyCompMeth	Key Compilation Method
KeyNo	Key Reference Number
KeyNoCEK	Key Reference Number of Change Entry Key
KeyNoCKUC	Key Reference Number to change the current KUC Entry
KeyNoM	Key Reference Number of MIFARE Key
KeyV	Key Version
KeyVa	Key (Version a)
KeyVb	Key (Version b)
KeyVc	Key (Version c)
KeyVCEK	Key Version of Change Entry Key
KeyVCKUC	Key Version to change the current KUC Entry
KeyVM	Key Version of MIFARE Key
KST	Key Storage Table (the place where the SAM stores the symmetric keys and their configuration)
KST	Key Storage Table
KUC	Key Usage Counter
LC	Logical Channel (the ISO-7816 concept)
LFI	Last Frame Indicator
LoadReg	Number of Register Value Set to be loaded
LRC	Longitudinal Redundancy Check
LSB	Least Significant Byte
MAC	Message Authentication Code
MAD	MIFARE Application Directory
MFP	MIFARE Plus
MGF	Mask Generation Function
MSB	Most Significant Byte
NumCards	Number of Cards
OAEP	Optimal Asymmetric Encryption Padding
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Card
PKI	Public Key Infrastructure
PKI_KST	The asymmetric counterpart of the KST: for storage of the PKI keys and their configuration.
PPS	Protocol and Parameter Selection
ProMas	Programming Mask
PSS	Probabilistic Signature Scheme

Table 22. Abbreviations *...continued*

Acronym	Description
RATS	Request for Answer To Select
RefNoKUC	Reference Number of Key Usage Counter
RegAddress	Register Address
RegContent	Register Content
REQA	Request Command, Type A
RFU	Reserved for Future Use
RndA	Random Number A
RndA'	Random Number A rotated left over 1 byte
RndB	Random Number B
RndB'	Random Number B rotated left over 1 byte
RSA	asymmetric cryptography
RSAES-OAEP	improved encryption/decryption scheme; based on the Optimal Asymmetric Encryption Padding scheme
RSA-OAEP	Asymmetric cryptography based on Optimal Asymmetric Encryption Padding for key agreement
RSASSA-PSS	improved probabilistic Signature Scheme with Appendix; based on the Probabilistic Signature Scheme
SAC	Secure Authenticated Channel
SAK	Select AcKnowledge
SAM	Secure Application Module
MIFARE SAM AV2	One of the SAM use mode
SEL	Select Code
SET	Configuration Settings for KST Entry
SHA- 256	Secure hash algorithm
SHA-1	Secure hash algorithm
SHA-224	Secure hash algorithm
SL3	MIFARE Plus Security Level 3
SN	Serial Number
StoreReg	Number of Register Value Set to be stored
SW	Status Word
TDEA	Triple Data Encryption Algorithm
TRNG	True random number generator
UID	Unique IDentifier
Va	Version of Key a
Vb	Version of Key b
Vc	Version of Key c
WUPA	Wake-Up Command, Type A
XOR	Exclusive OR

12. References

[1] **Data sheet —** P5DF081 MIFARE SAM AV2 BU-ID Doc. No. 1645**

[2] **Application Note —** MIFARE DESFire; Implementation hints and example, BU-ID Doc. No. 0945**

[3] **ISO 14443-3 —** ISO/IEC14443-3:2008

[4] **ISO 14443-4 —** ISO/IEC14443-4:2008

[5] **Data sheet —** MF1PLUSx0y1 Mainstream contactless smart card IC for fast and easy solution development, BL-ID Doc. No. 1637**[1]

[6] **Data sheet —** MF1ICS50 Functional Specification, BU-ID Doc. No. 0010**

[7] **Data sheet —** MF1ICS20 Functional Specification, BU-ID Doc. No. 1322**

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

[9] **Data sheet —** MF3ICD81 MIFARE DESFire Functional Specification, BU-ID Doc. No. 1340**

[10] **Data sheet —** MF0ICU1 Functional Specification, BU-ID Doc. No. 0286**

[11] **Data sheet —** MF0ICU2 Functional Specification, BU-ID Doc. No. 1376**

[12] **DES —** Data Encryption Standard (DES), NIST FIPS PUB 46-3, October1999, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[13] **User manual —** MF3ICD81 Guidance, Delivery and Operation Manual, BU-ID Doc No. 1469**

[14] **Wafer specification —** P5CD016/021/041 and P5Cx081 family, BU-ID Doc No. 1561**

[15] **PKCS1 —** PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, June 2002

[16] **SHA —** FIPS 180-2: Secure Hash Standard (SHS) – Current version of the Secure Hash Standard (SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512), 1 August 2002, amended 25 February 2004, FIPS Publication

[17] **ISO7816-2 —** ISO/IEC 7816-2:2002

[18] **ISO7816-3 —** ISO/IEC 7816-3:2002

[19] **ISO7816-4 —** ISO/IEC 7816-4:2004

[20] **AES —** FIPS197

[21] **ISO 10116 —** ISO/IEC 10116 block cipher

[22] **CMAC —** Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, May 2005, http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf

[23] **CMAC Errata —** Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, Errata, http://csrc.nist.gov/publications/nistpubs/800-38B/Updated_CMAC_Examples.pdf

1. ** ... document version number

[24] **BC-Methods —** Recommendation for Block Cipher Modes of Operation - Methods and Techniques, NIST Special Publication 800-38A, December 2001, http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

[25] **NIST Special Publication 800-38A —** Recommendation for Block Cipher Modes of Operation: Methods and Techniques, 2001.

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

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

[28] **Recommendation for Block Cipher Modes of Operation: Methods and Techniques —** FIPS PUB 197 ADVANCED ENCRYPTION STANDARD

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

[30] **AES —** Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST Special Publication 800-67, May 2008, http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf

13. Revision history

Table 23: Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
P5DF081_SDS v.3.2	20131217	Product short data sheet	-	P5DF081_SDS v.3.1
Modifications:	• Figure 3 “Pin configuration HVQFN32”: Remark added • Section 12 “References”: updated			
P5DF081_SDS v.3.1	20121001	Product short data sheet	-	P5DF081_SDS v.3.0
Modifications:	• Section 7.1 “Pinning”: updated			
P5DF081_SDS v.3.0	20111018	Product short data sheet	-	P5DF081_SDS v.1.0
Modifications:	• Section 1 “General description” and Section 5 “Ordering information”: updated • “RC522” updated with “RC52x or RC663” • Data sheet status changed into “Product short data sheet”			
P5DF081_SDS v.1.0	20100812	Objective short data sheet	-	-

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. 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.

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.

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.

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

DESFire — is a trademark of NXP B.V.

SmartMX — 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: 17 December 2013
191732

OCEAN CHIPS
Океан Электроники
Поставка электронных компонентов

Компания «Океан Электроники» предлагает заключение долгосрочных отношений при поставках импортных электронных компонентов на взаимовыгодных условиях!

Наши преимущества:

- Поставка оригинальных импортных электронных компонентов напрямую с производств Америки, Европы и Азии, а так же с крупнейших складов мира;
- Широкая линейка поставок активных и пассивных импортных электронных компонентов (более 30 млн. наименований);
- Поставка сложных, дефицитных, либо снятых с производства позиций;
- Оперативные сроки поставки под заказ (от 5 рабочих дней);
- Экспресс доставка в любую точку России;
- Помощь Конструкторского Отдела и консультации квалифицированных инженеров;
- Техническая поддержка проекта, помощь в подборе аналогов, поставка прототипов;
- Поставка электронных компонентов под контролем ВП;
- Система менеджмента качества сертифицирована по Международному стандарту ISO 9001;
- При необходимости вся продукция военного и аэрокосмического назначения проходит испытания и сертификацию в лаборатории (по согласованию с заказчиком);
- Поставка специализированных компонентов военного и аэрокосмического уровня качества (Xilinx, Altera, Analog Devices, Intersil, Interpoint, Microsemi, Actel, Aeroflex, Peregrine, VPT, Syfer, Eurofarad, Texas Instruments, MS Kennedy, Miteq, Cobham, E2V, MA-COM, Hittite, Mini-Circuits, General Dynamics и др.);

Компания «Океан Электроники» является официальным дистрибьютором и эксклюзивным представителем в России одного из крупнейших производителей разъемов военного и аэрокосмического назначения «**JONHON**», а так же официальным дистрибьютором и эксклюзивным представителем в России производителя высокотехнологичных и надежных решений для передачи СВЧ сигналов «**FORSTAR**».

AVIC JONHON

«JONHON» (основан в 1970 г.)

Разъемы специального, военного и аэрокосмического назначения:

(Применяются в военной, авиационной, аэрокосмической, морской, железнодорожной, горно- и нефтедобывающей отраслях промышленности)

«FORSTAR» (основан в 1998 г.)

ВЧ соединители, коаксиальные кабели, кабельные сборки и микроволновые компоненты:

(Применяются в телекоммуникациях гражданского и специального назначения, в средствах связи, РЛС, а так же военной, авиационной и аэрокосмической отраслях промышленности).

FORSTAR®

Телефон: 8 (812) 309-75-97 (многоканальный)
Факс: 8 (812) 320-03-32
Электронная почта: ocean@oceanchips.ru
Web: http://oceanchips.ru/
Адрес: 198099, г. Санкт-Петербург, ул. Калинина, д. 2, корп. 4, лит. А