P5DF072EV2/T0PD4090

MIFARE SAM AV1

Rev. 3.1 — 14 June 2010
189731

Product short data sheet
PUBLIC

1. General description

NXP Semiconductors have developed the MIFARE SAM AV1 (Secure Application Module) for use with readers and terminals that have a smartcard slot for contact smartcards supporting ISO/IEC 7816 class A, class B and class C. The transport protocol complies with ISO/IEC 7816-3 (T=1 protocol). Instructions are coded according to ISO/IEC 7816-4.

Secured communication

When used in combination with a reader IC supporting innovative "X" features, MIFARE SAM AV1 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 connection between the SAM and the reader is performed using security protocols based on symmetric cryptography (TDEA and AES).

2. Features and benefits

2.1 Cryptography

- Supports MIFARE Crypto1, TDEA (Triple DES encryption algorithm) and AES cryptography
- Supports MIFARE 1K, MIFARE 4K, MIFARE DESFire, MIFARE DESFire EV1
- Secure storage of keys (key usage counters)
- 128 key entries for symmetric cryptography
- Key diversification

2.2 Communication

- Up to four logical channels; simultaneous multiple card support
- Secure host ↔ SAM and back end ↔ SAM communication with symmetric cryptography 3 pass authentication for confidentiality and integrity
- Supports high speed baud rates up to 1.5 Mbit/s
- Supports ISO 7816 baud rates
- True Random Number Generator (TRNG)

2.3 Delivery types

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

3. Applications

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

4. Quick reference data

Table 1. Quick reference data

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
P5DF072EW1/T0PD4090	FFC	8 inch wafer (sawn; 150 μm thickness; on film frame carrier; electronic fail die marking according to SECSII format)	not applicable
P5DF072EV2/T0PD4090	PCM1.1	contact chip card module (super 35 mm tape format, 8-contact)	SOT658-1
P5DF072EHN/T0PD4090	HVQFN32	plastic thermal enhanced very thin quad flat package; no leads; 32 terminals; body 5 x 5 x 0.85 mm	SOT617-3

6. Block diagram

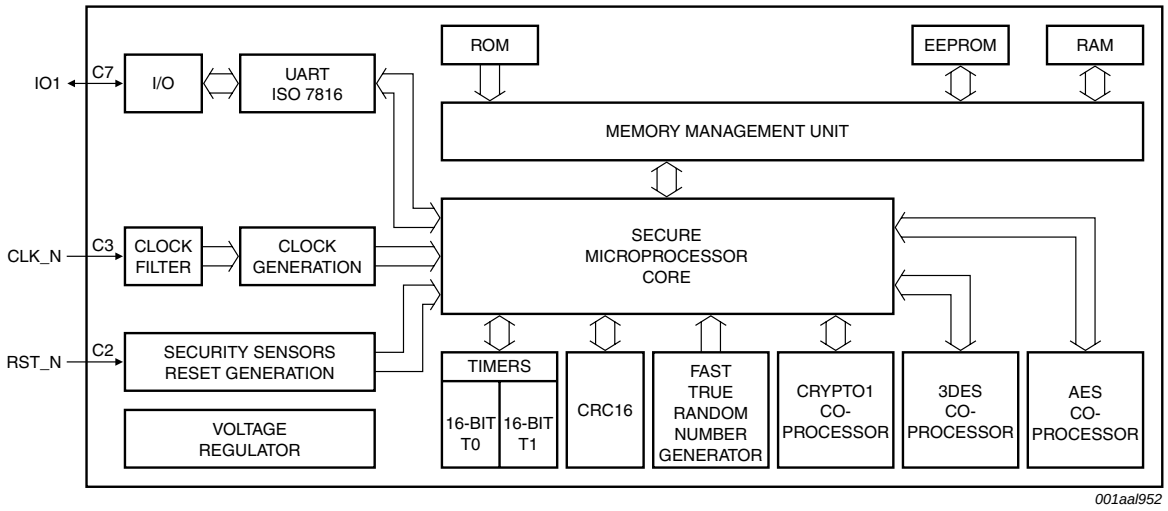

Fig 1. Block diagram

7. Functional description

7.1 Contact interface

The pad assignment and the electrical characteristics are fully compliant with ISO/IEC 7816 (part 2 and part 3). The MIFARE SAM AV1 operates with class A, class B and class C 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 I^2C-bus communication to the MFRC52X reader chip. Pad C8 is used as the data line to the reader chip. These two pads for connection to the MFRC52X are the only ones deviating from the ISO standard pin assignment.

7.2 External clock frequency and bit rates

The basic operating frequency of the MIFARE SAM AV1 is 3.5712 MHz. With this frequency the standard bit rates can be reached using ISO/IEC 7816 transmission factors F and D.

The maximum specified bit rate in all cases is 1.5 Mbit/s.

7.3 UID/serial number

The SAM 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.

The UID can be obtained by using the SAM_GetVersion command.

7.4 Cryptography and key handling

7.4.1 DES and 3DES cryptography

Both DES and 3DES keys consisting of 112 bits are stored in strings of 16 bytes; 3DES keys consisting of 168 bits are stored in strings of 24 bytes.

7.4.2 AES cryptography

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 with 16 bytes. Therefore data streams are always padded to lengths that are multiples of 16 bytes.

All cryptographic operations are done in cipher block chaining mode, which defines the result of the previous operation to be the init vector of the next cryptographic operation. For sending data the CBC send mode is applied, for receiving it is always CBC receive mode.

7.4.3 MIFARE cryptography

MIFARE keys are stored in the same space as AES and 3DES keys using the following scheme:

- MIFARE standard key A in byte 0 to byte 5 of the 16 byte field
- Key number (KeyNo) of the MIFARE standard key diversification key for MIFARE key A in byte 6 of the 16 byte field
- Key version of the MIFARE standard key diversification key for MIFARE key A in byte 7 of the 16 byte field
- MIFARE standard key B in byte 8 to byte 13 of the 16 byte field
- KeyNo of the MIFARE standard key diversification key for MIFARE key B in byte 14 of the 16 byte field
- Key version of the MIFARE standard key diversification key for MIFARE key B in byte 15 of the 16 byte field

Remark: MIFARE key versions can only be stored for a key pair A and B.

7.4.4 Key versioning

The MIFARE SAM AV1 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, 3DES, 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.

7.4.5 Key diversification mechanisms

A main feature of the MIFARE SAM AV1 allows diversification of any kind of keys (AES, DES, 3DES and MIFARE).

The following diversification mechanisms are implemented:

- Diversification of MIFARE keys using a 3DES key
- Diversification of 3DES keys using the key to diversify itself
- Diversification of AES keys using the key to diversify itself

7.4.6 Key storage

The MIFARE SAM AV1 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 (3)DES, two 3key3DES, three AES128, two AES192 or six MIFARE keys plus their attributes.

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

7.4.6.1 Key reference number

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

KeyNo 00h is defined as the SAM master key:

- The three/two key versions stored in KeyNo 00h are used for host authentication after reset in case bit 10 of the configuration settings SET of key 00h is set to logic 1

7.4.7 Key usage counters

In order to count and limit the number of authentications a key entry can be used for, MIFARE SAM AV1 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.

7.4.7.1 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.

7.4.7.2 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.

If the limit is changed to a value lower than the current value, the usage of all key entries linked to this counter is prohibited.

7.4.7.3 Key reference number to change the current KUC entry

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

7.5 MIFARE SAM AV1 command set

7.5.1 SAM configuration commands

SAM_DisableCrypto

This command allows the permanent and irreversible disabling of the cryptographic functionality of the SAM.

7.5.2 SAM key handling commands

SAM_ChangeKeyEntry

This command updates any key entry of the KST.

SAM_GetKeyEntry

The SAM_GetKeyEntry command allows reading the contents of the key entry specified in the parameter KeyNo.

SAM_ChangeKUCEntry

This command updates any key usage counter entry stored in the MIFARE SAM AV1. Always the limit, KeyNoCKUC and KeyVCKUC have to be sent.

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_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 SAM prior to issuing this command.

SAM_DumpSessionKey

The command SAM_DumpSessionKey can be used to retrieve the session key generated by the SAM.

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.

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.

SAM_ChangeKeyMIFARE

This command is intended to change a key in a MIFARE card. The command allows:

- a prepared encrypted stream to be written to a MIFARE 1K or 4K card containing the desired keys and the given access conditions
- reading out a single MIFARE key to be used for any kind of MIFARE transaction in a host system directly

In the latter case, the key can be retrieved encrypted from the SAM 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.

7.5.3 SAM security related commands

SAM_AuthenticateHost

The command SAM_AuthenticateHost is used to run a mutual 3-pass authentication between the SAM and host system.

SAM_SelectApplication

The command SAM_SelectApplication is the equivalent of the SelectApplication command of DESFire. The SAM generates a list of available keys linked to the specified Application ID as defined in the key entry property ‘DF_AID’.

SAM_AuthenticatePICC

In this procedure both the PICC as well as the SAM 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_LoadInitVector

The command SAM_LoadInitVector is used to load an init vector for the next cryptographic operation into the MIFARE SAM AV1.

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_AuthenticateMIFARE

In this procedure, both the MIFARE card as well as the SAM device show in an encrypted way that they possess the same secret which especially means the same key.

SAM_KillAuthentication

Invalidates any kind of authentication in the logical channel the command is issued.

SAM_IsoAuthenticatePICC

In this procedure both the PICC as well as the SAM 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 operate 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.

SAM_IsoGetChallenge

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 SAM internally is set into a state indicating that an authentication procedure is ongoing. Consequently, the command that is called after getting the random number is aborted (except SAM_IsoExternalAuthenticate). After aborting, the SAM 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 subsequently without interrupting the sequence by another command.

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 SAM.

Such an authentication proves that both the SAM and the host contain the same secret, namely a DES, 3DES 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 SAM.

Such an authentication proves that both the SAM and the host contain the same secret, namely a DES, 3DES or AES key, and generates a session key for further cryptographic operations.

7.5.4 SAM data processing commands

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.

To do so, the plain data is enciphered in cipher block chaining send mode. Padding bytes (if applicable) are generated internally for cryptographic operation.

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.

To do so, the plain data is enciphered in cipher block chaining send mode. Padding bytes (if applicable) are appended automatically for cryptographic operations but are not transmitted.

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.

To do so, the plain data is deciphered in CBC receive mode. CRC and padding bytes are checked for validity automatically.

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 enciphered in cipher block chaining send mode. CRC and padding bytes are appended automatically.

7.5.5 SAM general commands

SAM_GetVersion

The SAM_GetVersion command returns manufacturing related data of the SAM.

7.5.6 SAM power saving commands

SAM_Sleep

Forces the SAM to put a connected MFRC52X into sleep mode and itself into idle mode to reduce power consumption.

The SAM will answer the command and afterwards switch to idle mode.

7.5.7 MFRC52X control commands

RC_ReadRegister

Read the content of one or more register(s) of the connected reader chip.

The command allows the reading of 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.

The SAM does not check if the address of the MFRC52X is a valid register address.

RC_WriteRegister

Write the content of one or more register(s) of the connected reader chip.

The command allows the writing to 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.

The SAM will not check if the address of the MFRC52X is a valid register address.

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 SAM to wait this additional time until turning on the field again.

The unit for the time value is milliseconds.

RC_Init

Establishes the serial connection between SAM and MFRC52X and initializes the reader chip with the register values stored in the selected register value set.

RC_LoadRegisterValueSet

Stores a customer defined register value set for the MFRC52X in the non-volatile memory of the SAM. This set can then be used for initializing the reader chip with the RC_Init command. The address and the related value for the register have to be placed consecutively in the command data field of the APDU.

A register value set can store a maximum of 31 initialization values.

7.5.8 ISO14443-3 type A card activation commands

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.

The selection can be carried out for a variable amount of cascade levels. The select codes have to be listed in the data field subsequently. The SAM will take the parameters exactly and use them as select code. Therefore to fully select a card with a triple UID, the data field has to be of three bytes length indicating 93h, 95h and 97h whereas the data field has to be of one byte length indicating 93h if a single size UID card is to be selected.

If the select code indicates a cascade level of 93h and 95h, and the UID of the card consists only of four bytes, the SAM exits the command and returns the SAK and the UID of the card.

If the select code indicates a cascade level of 93h, and the UID consists of more than four bytes, the SAM also exits the command and returns the SAK and the first three bytes of the UID but indicates with a special return code the incompleteness of the UID separately. The caller has then to take care about continuing the procedure on his own by calling the command once more with a higher select code. The UID bytes already returned will not be returned a second time. The same applies for a select code of 95h if the UID is of ten bytes length (suggest that a selection with code 93h is implemented first).

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 SAM takes the user data and sends it without changing, inserting or appending any content to the contactless card. Appending a CRC, time-out settings, etc. have to be configured by directly writing to the MFRC52X registers. Take into account that switching settings of the reader chip influence all subsequent SAM commands proposing the correct reader chip settings, i.e. ISO14443-4_Exchange.

7.5.9 MIFARE commands

MF_Authenticate

Performs an authentication with a MIFARE card. The MIFARE key has to be stored in the SAM 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 SAM 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 SAM accesses the blocks in the same order as addresses listed in the command data field. The command supports writing 16 bytes encrypted for MIFARE 1K and 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 SAM 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 SAM 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 SAM accesses the blocks in the same order as addresses listed in the command data field.

If incrementing of a block fails, the SAM returns the 4-bit status code of the MIFARE card in the lower nibble and the hexadecimal value ‘F’ in the higher nibble of the status byte SW2. No information about the block write error is provided. Be aware that some blocks may have been updated already.

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 SAM 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 SAM 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.

If copying of a block fails, the SAM returns the 4-bit status code of the MIFARE card in the lower nibble and the hexadecimal value ‘F’ in the higher nibble of the status byte SW2. No information about the block write error is provided. Be aware that some blocks may have been updated already.

MF_AuthenticateRead

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 SAM 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_AuthenticateWrite

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 SAM 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 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.

7.5.10 ISO14443-4 type A commands

ISO14443-4_RATS_PPS

Execute a combined RATS and PPS sequence to prepare a card for T=CL data exchange.

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.

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.

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.

7.5.11 DESFire related commands

DESFire_AuthenticatePICC

In this procedure both the PICC as well as the SAM 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. Be aware that this command may have some limitations, see Ref. 3.

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 SAM 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 SAM 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.

8. Limiting values

Table 3. 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	DC; on pads IO1, IO2 or IO3		-	±15.0	mA
I_O	output current	DC; on pads IO1, IO2 or IO3		-	±15.0	mA
I_{lu}	latch-up current	$V_I < 0$ V 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
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 to +85 °C.

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

9. Abbreviations

Table 4. Abbreviations

Acronym	Description
AES	Advanced Encryption Standard
AID	Application IDentifier
APDU	Application Protocol Data Unit
AppData	Application Data
ATR	Answer To Reset
ATS	Answer To Select
ATQA	Answer To reQuest, type A
Authent	Authentication
Auth mode	Authentication mode
CBC	Cipher Block Chaining
CID	Card IDentifier
CmdCode	Command Code
CmdSettings	Command Settings
CRC	Cyclic Redundancy Check
CurVal	Current Value of key usage counter
CWT	Character Waiting Time
DES	Data Encryption Standard

Table 4. Abbreviations *...continued*

Acronym	Description
DF_AID	DESFire AID
DF_KeyNo	DESFire Key Number
DFKeyNo	DESFire Key Number
Div	Diversification
DRI	Divisor Receive Integer
DSI	Divisor Send Integer
EEPROM	Electrically Erasable Programmable Read Only Memory
ekNo(x)	Encrypted Number 'x'
ek(x)	Encrypted '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
FSDI	Frame Size for Device Integer
FWI	Frame Waiting time Integer
INS	INStruction code
ISO	International Organization for Standardization
IV	Initial Vector
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
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
KUC	Key Usage Counter
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
MSB	Most Significant Byte
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Card
PPS	Protocol and Parameter Selection
ProMas	Programming Mask

Table 4. Abbreviations *...continued*

Acronym	Description
RATS	Request for Answer To Select
RefNoKUC	Reference Number of KUC
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
SAK	Select AcKnowledged
SAM	Secure Application Module
SEL	SELect code
SET	configuration SETtings for KST entry
SN	Serial Number
StoreReg	number of register value set to be stored
SW	Status Word
UID	Unique IDentifier
WUPA	Wake-UP command, type A
XOR	eXclusive OR

10. References

[1] **Data sheet —** P5DF072EV2/T0PD4090 MIFARE SAM AV1, BU-ID document number: 1297**[1]

[2] **Data sheet —** MF3ICD81 MIFARE DESFire functional specification, BU-ID document number: 1340**

[3] **Application Note —** MIFARE SAM AV1 - Features and hints, BU-ID document number: 1654**

[4] **Reader Software Library —** DESFire ev1 SAM library, BU-ID document number: 1553**

[5] **Demo Software —** MIFARE discover PC demo software for MIFARE SAM AV2, BU-ID document number: 1866**

1. ** document version number.

11. Revision history

Table 5. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
P5DF072EV2/T0PD4090_SDS_31	20100614	Product short data sheet	-	189730
Modifications:	• Minor text and standardization modifications			
189730	20100415	Product short data sheet	-	-

12. Legal information

12.1 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.

12.2 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.

12.3 Disclaimers

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

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

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

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

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

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

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

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

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

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

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

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

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

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

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

12.4 Licenses

ICs with DPA Countermeasures functionality

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.

12.5 Trademarks

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

I²C-bus — logo is a trademark of NXP B.V.

MIFARE — is a trademark of NXP B.V.

DESFire — is a trademark of NXP B.V.

13. Contact information

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

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

14. Contents

continued >>

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

Date of release: 14 June 2010
189731