AN12701

MIFARE SAM AV3 - Interface and Architecture

Rev. 1.1 — 9 January 2020 Application note
521111 COMPANY PUBLIC

Document information

Information	Content
Keywords	MIFARE SAM AV3, Secure Key Storage, TDEA, AES, RSA. Key Usage Counters.
Abstract	This application note explains the interface and architecture of MIFARE SAM AV3.

Revision history

Rev	Date	Description
1.1	20200109	AN number changed, security status changed into “Company Public”.
1.0	20190401	Initial version.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

1 Introduction

MIFARE SAMs (**S**ecure **A**pplication **M**odule) have been designed to provide the secure storage of cryptographic keys and cryptographic functions for the terminals to access the MIFARE products[1] securely and to enable secure communication between terminals and host (backend).

1.1 Scope

This application note describes different interface and architecture. There is a set of application note for MIFARE SAM AV3; each of them is addressing specific features. The list of application note is given in [6].

This application note is a supplement document for application development using MIFARE SAM AV3. Should there be any confusion please check MIFARE SAM AV3 function specification [1]. Best use of this application note will be achieved by reading this specification [1] in advance.

Note: This application note does not replace any of the relevant functional specifications, data sheets, application notes or design guides.

1.2 Abbreviation

Refer to Application note “MIFARE SAM AV3 – Quick Start up Guide” [6].

1 MIFARE Ultralight C, MIFARE Classic, MIFARE Plus, MIFARE DESFire, MIFARE DESFire EV1

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

2 MIFARE SAM AV3 Interface

MIFARE SAM AV3 offers ISO/IEC 7816-3 standard contact interface to the host or microcontroller and I^2C interface to RC52x, PN51x and RC66x. MIFARE SAM AV3 pinning information is given in [1].

In addition to that, the MIFARE SAM AV3 also supports a I2C Slave interface instead of the ISO7816-3 contact interface. This is only available on MIFARE SAM AV3 in HVQFN32 package.

2.1 Host (microcontroller) Interface to SAMs

MIFARE SAM AV3 supports the contact communication speed up to 1.5 Mbps, which is not achievable by using standard 7816 UART-based reader.

2.1.1 Standard ISO/IEC 7816 Communication

Any standard ISO/IEC 7816 reader can be used to communicate with MIFARE SAM AV3. In this case, the transmission speed is limited (standard 9600 bps and during communication 115200 bps are commonly used) to ISO/IEC 7816-3.

In a standard reader, any standard framework can be used to access MIFARE SAM AV3, e.g., the standard PC/SC framework. The built-in Windows Application Program Interface (API) 'winscard' can establish the communication between the application and MIFARE SAM AV3. The following diagram shows this type of communication:

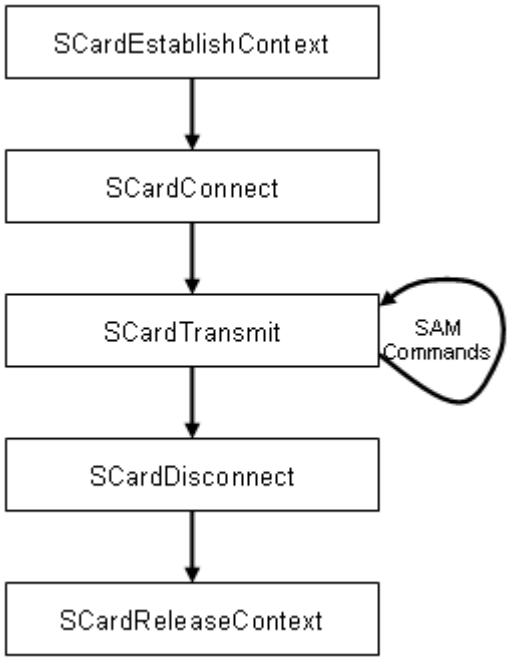

Figure 1. Flow diagram of accessing MIFARE SAM AV3 in PC/SC framework

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

2.1.2 Higher communication speed implementation

According to ISO/IEC 7816, it is not possible to take advantage of the very high speed (**1.5 Mbps**) interface, which is one of the strengths of NXP SAMs. Moreover, the very complex error handling of the block-oriented T=1 protocol makes a high-speed implementation very complicated. Therefore, we recommend using an optimized non-ISO 7816 protocol for the Microcontroller to SAM communication.

When using a standard microcontroller with 3 V or 5 V VCC, the connection of the VCC and GND signals is straightforward, because SAM *supports* Class B (3 volt nominal) and Class A (5 volt nominal) refer to ISO/IEC 7816 part 3. The same approach is applicable for the RST pin. It is connected to an I/O-Pin at the microcontroller.

For S-mode only, also 1.8 V (Class C) is supported.

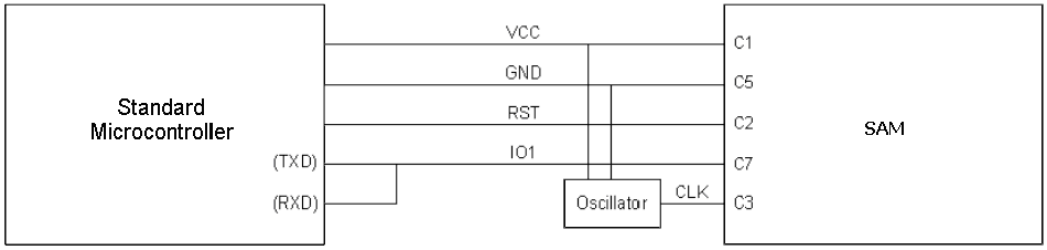

Figure 2. SAM Interface

VCC and GND pin are connected respectively to the supply power for SAM. The RST pin (C2) of SAM is connected to a general-purpose I/O-Pin of the microcontroller. Generation of the clock is performed by an external oscillator.

The diagram below shows the typical activation sequence. The time TS – TC could alternatively be zero. Because SAM (Smart Card ICs) needs a time for its internal boot sequence (hardware and security checks), it is necessary that the RST signal is held low (TS-TR) for approximately 1 ms after switching VCC (VDD) on.

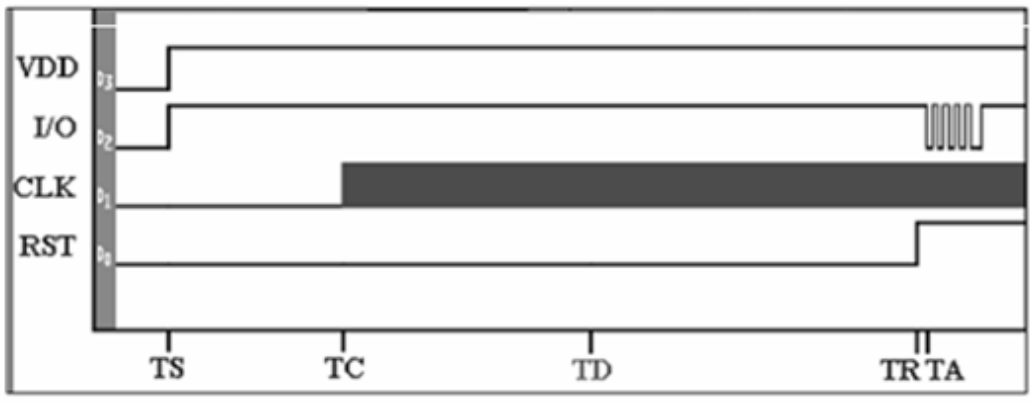

Figure 3. Typical activation signals for SAM

To realize the serial communication, the two separate serial communication lines of the microcontroller (full duplex serial port) have to be merged to a single receive/transmit line (half-duplex serial port). If the microcontroller provides appropriate functionality on its I/O-Pins, it is possible to avoid supplementary hardware. It is essential that the pins of the microcontroller are configured as input or output. There should also be a possibility to connect a pull-up or pull-down resistor to a pin. This could be done on a standard 8051 microcontroller by writing to the corresponding registers.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

Switching the general-purpose pins to serial input and serial output is also performed by setting a register correctly [see detail in your microcontroller data sheet]. Therefore it is possible to connect the pins in parallel and to change the pin circuitry by software. The solution for implementing an error-free data transmission using only one I/O line leads to the transmission modes described as follows (see also figure below):

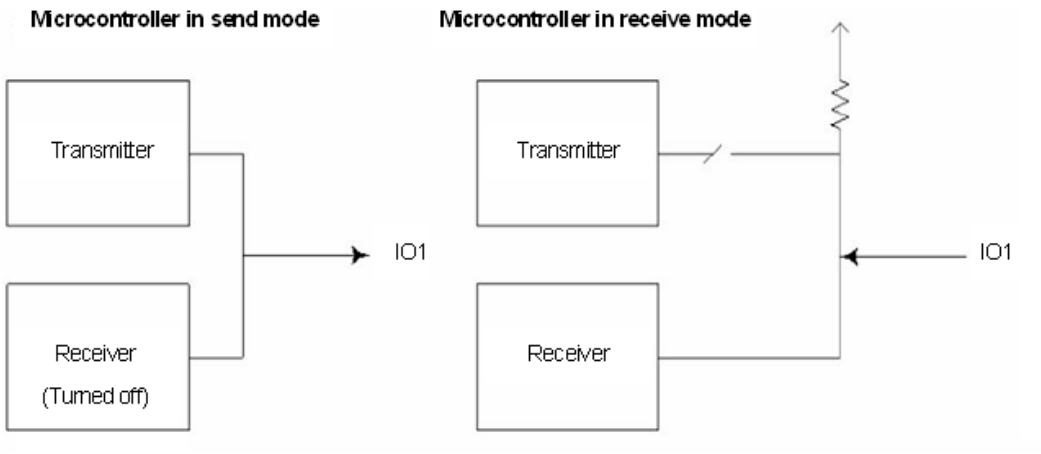

Figure 4. Serial Communication

Microcontroller in send mode: The receiver is turned off, so that no data which has been sent is looped back and detected by the receiver of the microcontroller.

Microcontroller in receive mode: The transmitter is also turned on, but the port pin is disconnected from the transmitter, configured as an input pin and pulled up via its internal pull-up resistor. Thus, the output is forced to high if no data is sent by the Smart Card IC (as demanded by ISO/IEC 7816-3 to signal idle status). If the Smart Card IC sends data, the input follows the applied signal.

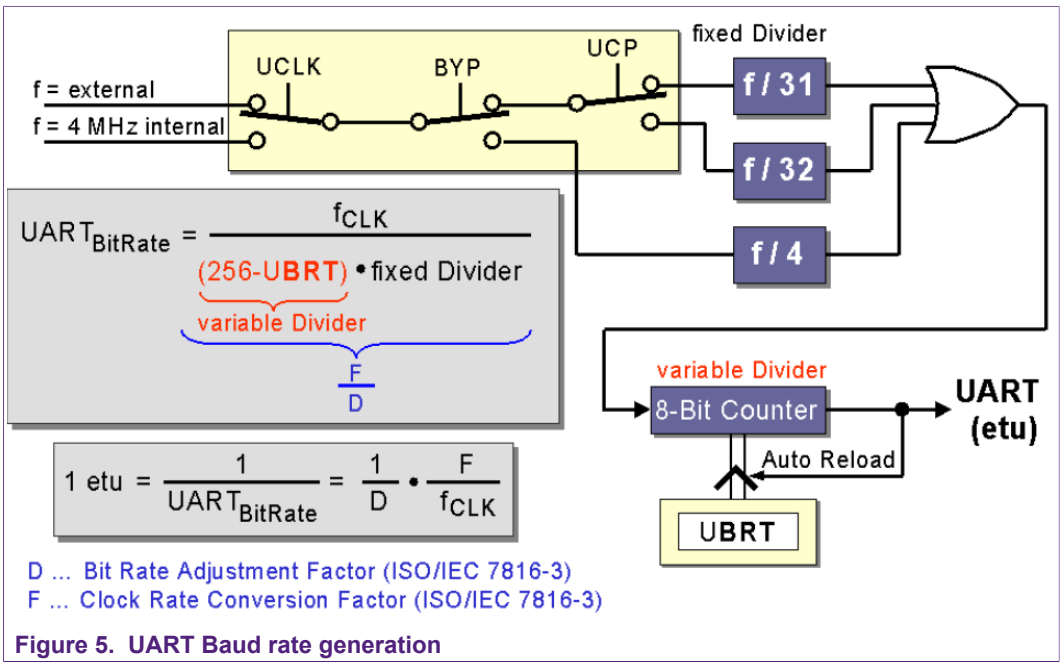

Figure 5. UART Baud rate generation

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

The configuration of baud rates is performed by ration programming. In order to achieve the baud rates the external or the internal 4 MHz signal is to be divided via - variable Divider (Auto-reload value of the Baud rate Timer) in conjunction with pre-scaled division factor 31, 32 or 4. The minimum time for 1 etu is defined by the internal UART design to 8 clock cycles. Thus, any configuration of the Baud Rate Generator should consider this value as a limit for reliable operation. Consequently, a Baud Rate Timer reload value of 255 (0xFF) may not be used, if a UART prescaler divisions factor of 4 is selected. All baud rate configurations are controlled by the Special Function Registers:

- UART Control Register UCON

- Baud Rate Timer Reload Register UBTR.

The baud rate timer is an 8-bit up-counter with auto-reload at each overflow. UART control bit RUN in SFR UCON switches both the UART core and the Baud rate Timer on (RUN=1) and off (RUN=0). A 0-to-1 transition of control bit RUN loads the UBTR value to the internal counter. Thus UBTR also provides the initial counter preload value.

2.1.3 Logical Channels

SAM supports four logical channels separated by a hardware firewall. These logical channels can be distinguished using the bits b1b0 of class byte.

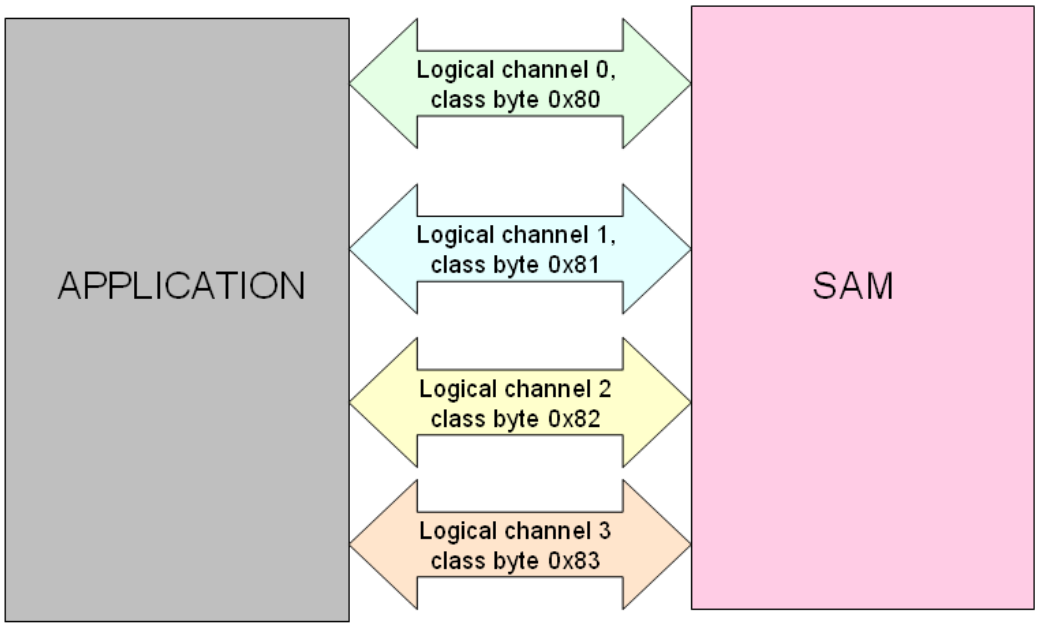

Figure 6. Four logical channels in SAM

Different logical channels can be used for different purposes. As example:

- four logical channels for four different MIFARE DESFire cards activated in the field
- One channel can be used for calculation of crypto using an Offline Crypto Key and second channel for calculation of crypto using PICC authentication.

The logical channels cannot be used to issue commands in parallel but can be used one by one per command (still making it possible to execute independent transactions in parallel). Notice that there are some additional restrictions as execution of chained commands or a security protocol (authentications, proximity checking) on one logical channel also needs completion before the other logical channels can be addressed

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

again. In MIFARE SAM AV3 logical channel's communications to the host are secured per channel (examples are given in "MIFARE SAM AV3 – Host Communication" application note)."

There are two limitations:

- Only one active MIFARE Classic authentication at a time is supported by MIFARE SAM AV3.
- When multi-part commands (like authentication commands or chained commands) are performed on an LC, the parallel processing on the LCs is serialized. In other words, all LCs except the one on which the multi-part command is requested are unusable until the multi-part command is performed to its end.

2.1.4 I2C Slave interface

As an alternative to the UART-based ISO 7816 T=1 communications, the SAM AV3 supports an I2C Slave interface to replace the ISO 7816-3 low-level UART character transmission. The I2C Slave interface supports the existing ISO 7816 block interface. The I2C slave interface is compatible with the I2C standards for transmission and reception of bits, bytes and blocks as detailed in the I2C-bus specification [2]. The major difference between ISO7816 and I2C is that the ISO7816 interface is asynchronous and the SAM AV3 can send a response at any time up to the BWT after receiving a T=1 command from the Host. For I2C Slave the communication is synchronous, therefore the SAM AV3 can only return data as part of a READ request from the Host Master.

Details about the I^2C Slave interface can be found in [4].

2.2 I2C Interface to RC52x, PN51x, or RC66x for X-Connection

The I^2C interface has to be implemented as described in [2]. The Slave address of the frontend is fixed and known by the SAM. The I^2C communication speed is up to 400 kbps.

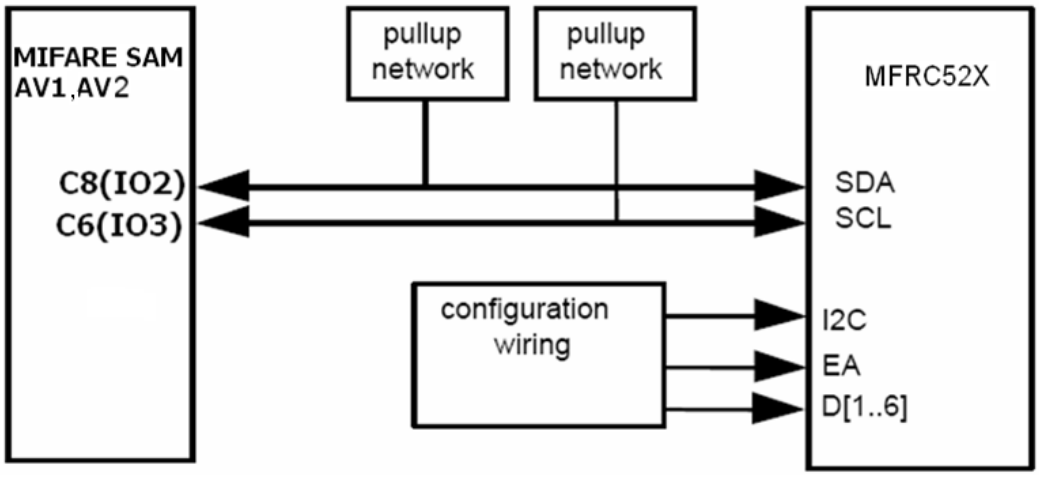

Figure 7. I^2C Interface

Detail I^2C specification can be found in [3].

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

3 MIFARE SAM AV3 Functional Types

MIFARE SAM AV3 can be used in two ways: S-Mode and X-Mode.

3.1 S-Mode

In this way, microcontroller is controlling the communication among SAM, Backend (if any) and contactless card.

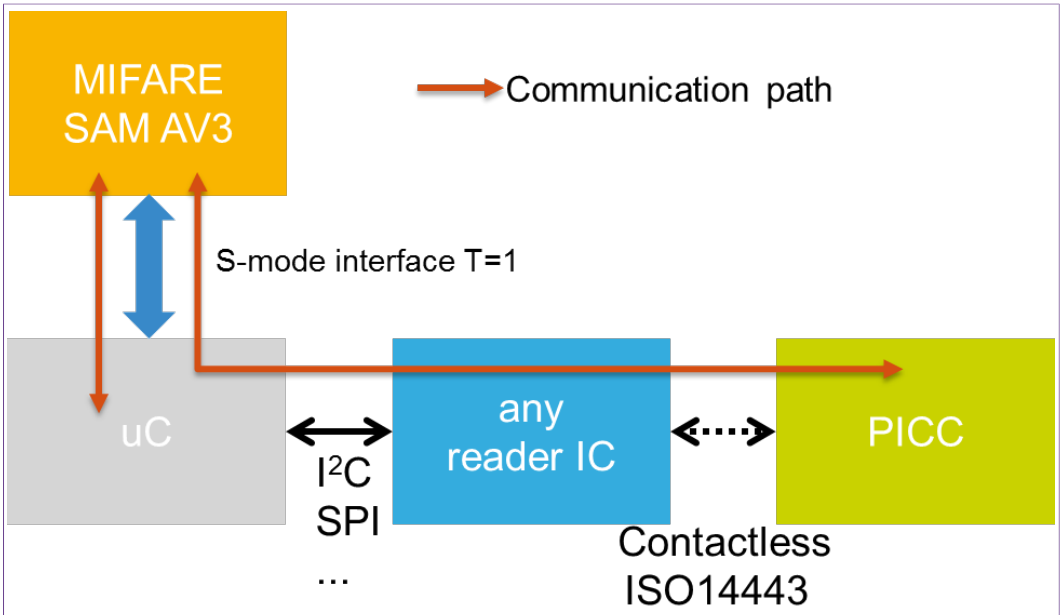

Figure 8. Non X-Connection architecture

The communication path is longer and can be slower. For example, MIFARE DESFire EV2 Authentication is shown in the following figure.

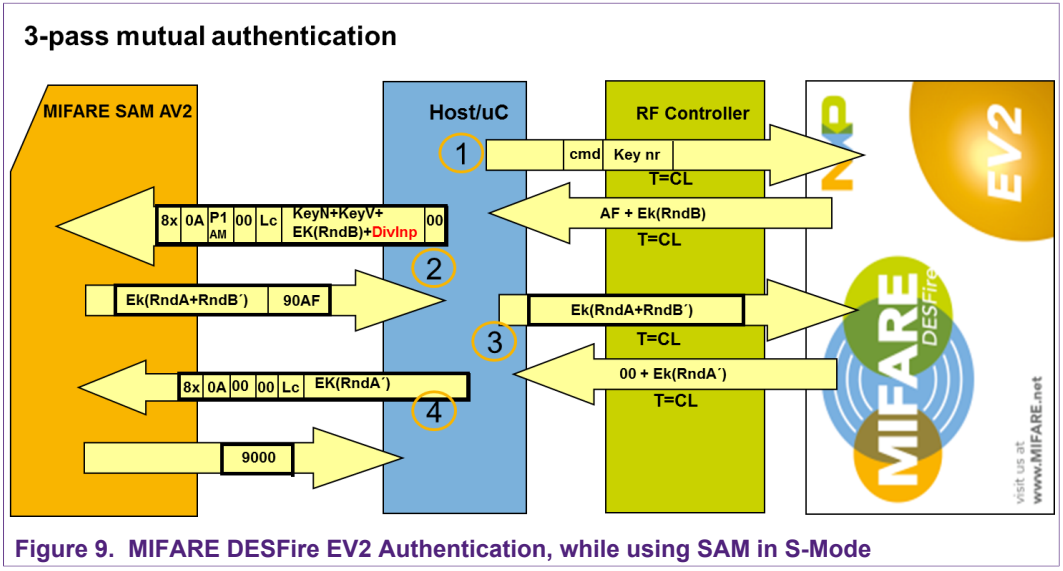

Figure 9. MIFARE DESFire EV2 Authentication, while using SAM in S-Mode

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

3.2 X-Mode

The SAM is connected directly to the contactless reader IC RC52x, PN51x or RC66x.

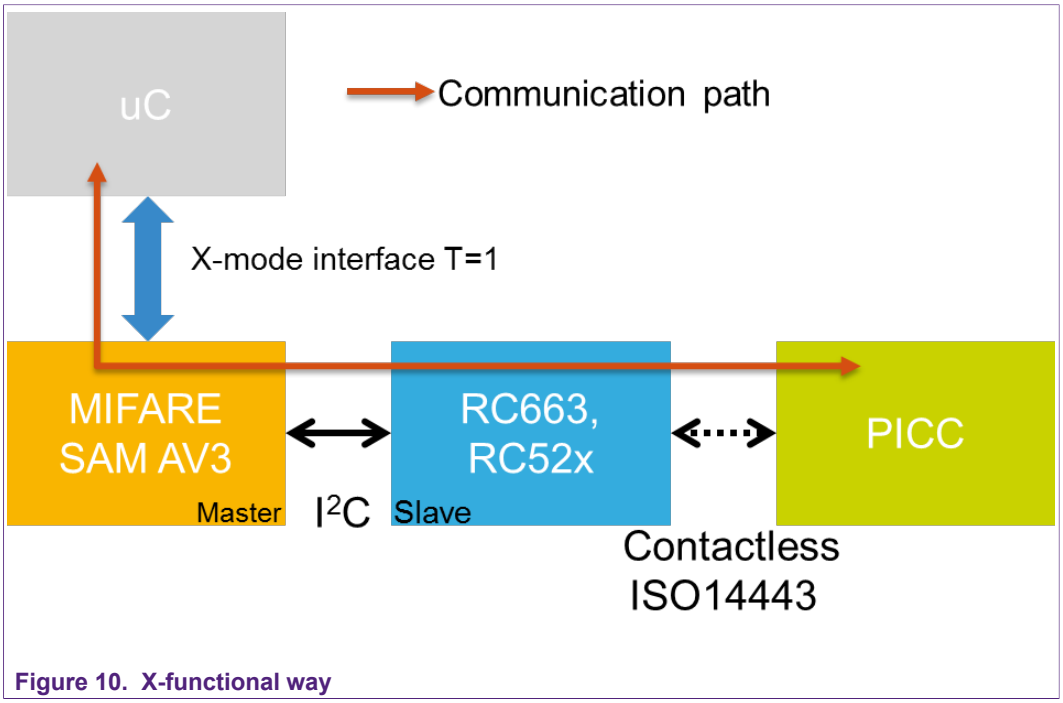

Figure 10. X-functional way

In this case µC just send command to the SAM, SAM is doing everything by himself. The communication path is shorter and faster. For example, MIFARE DESFire EV2 Authentication is shown in the following figure.

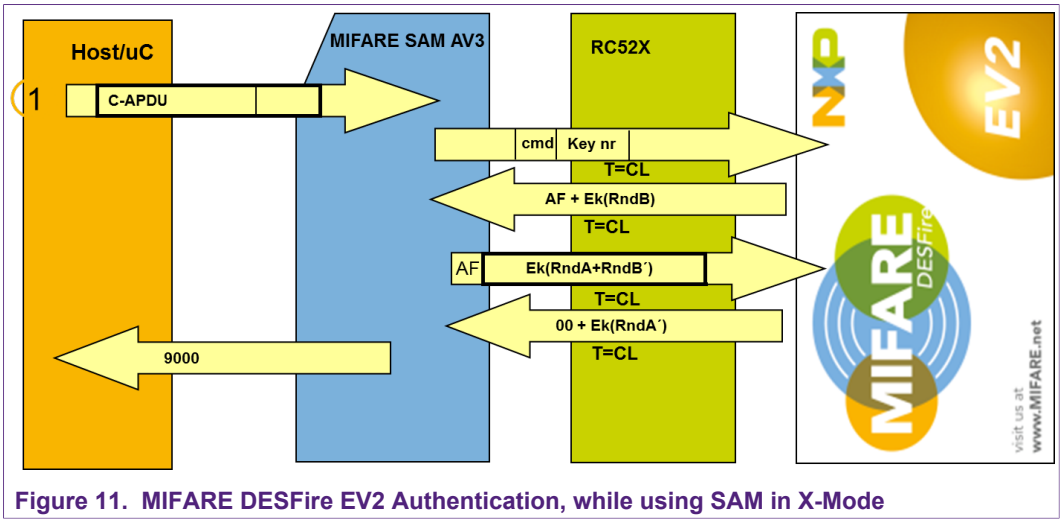

Figure 11. MIFARE DESFire EV2 Authentication, while using SAM in X-Mode

It is possible to use SAM also in S-Mode way while connected in X-Mode way. The X-Mode is described in MIFARE SAM AV3 – X functionalities application note, doc nr. 1829xx.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

4 MIFARE SAM AV3 Architectures

MIFARE SAM AV3 is a secure controller chip with secure storage of the cryptographic keys and counter. It has hardwired crypto co-processors for MIFARE Crypto 1, TDEA, AES, RSA, ECC and hash functions.

The following figure shows different crypto algorithms and their usages, supported by MIFARE SAM AV3.

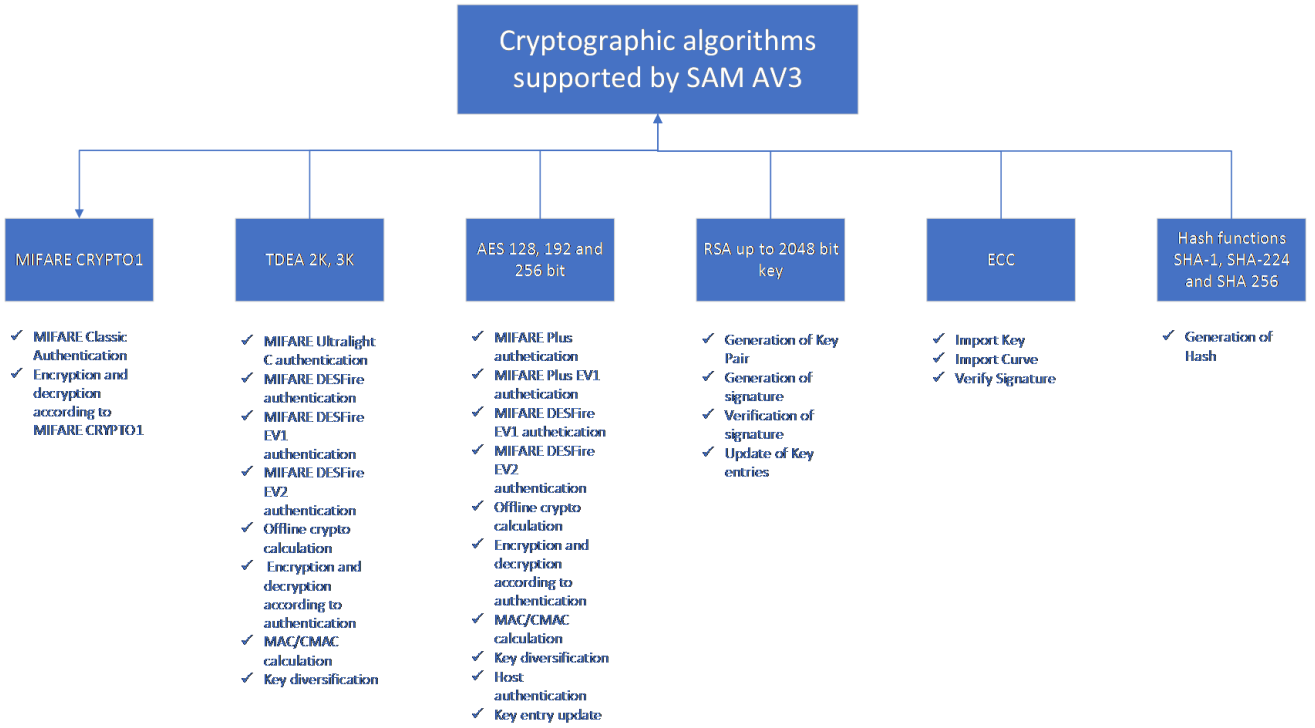

Figure 12. MIFARE SAM AV3 cryptographic algorithms and usages

Moreover, MIFARE SAM AV3 clearly classifies the key usages class. See detail in § 4.2.11. One type of “key class” can be used only for specific type of cryptographic calculation.

4.1 MIFARE SAM AV3 Storage

MIFARE SAM AV3 user memory can be logically described using the following tables.

1. Symmetric Key Storage Table (sKST)
2. PKI Key Storage Table (PKI_KST)
3. Last Recently Used keys (LRU) table
4. Key Usage Counter (KUC)

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

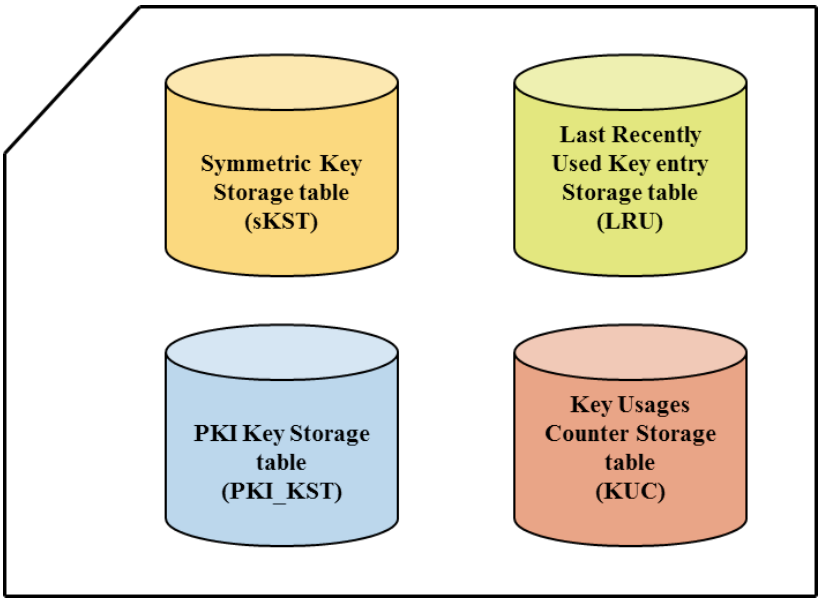

Figure 13. MIFARE SAM AV3 storage

Different storage tables are described in the following sections.

4.2 Symmetric Key Storage Table (sKST)

The symmetric key storage table holds a maximum of 128 entries. Each entry has 48 bytes storage for a key value. For 16-byte keys these 48 bytes can be considered as three positions of 16-byte each; correspondingly, for 24-byte keys these 48 bytes can be considered as two positions of 24-byte each. The keys can be downloaded (updated) over a protected link and can never be read from the MIFARE SAM AV3. They are used only internally to the SAM for the cryptographic operations. The elements of symmetric key storage table are described as follows:

Byte	0 15	16 31	32 47	48 49 50	51	52	53	54	55 56	57	58	59	60 61	62	63
Key entry nr.	KeyVa	KeyVb	KeyVc	DF_AID	DF_KeyNo	KeyNoCEK	KeyVCEK	REFNoKUC	SET	Va	Vb	Vc	ExtSET	KeyNoAEK	KeyVAEK
0															
1															
2															
..	KeyVa 24byte		KeyVb 24byte												
..	KeyVa 32 Byte														
127															

Figure 14. MIFARE SAM AV3 Symmetric Key storage table components

To address a key from the key entry table, two parameters are required, the key entry number (0 to 127) and the version number (0 – 255). See the example, addressing key from the SAM. For the purposes of authentication, it is the key version that determines exactly which key will be used from the key entry. When the sKST is accessed with an entry number and a key version, SAM searches within the three positions A, B and C for the key entry with the matching version number; it then uses that key. If two positions contain different keys with the same version number, only the first occurrence will be used.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

4.2.1 KeyNo: Key Reference number

The key reference number, ranging from 0 to 127, refers to an entry in the sKST. Entry 0 is defined as the MIFARE SAM AV3 master key.

4.2.2 PosA: Position for key version A

16 bytes for 16-byte TDEA or AES key and also for MIFARE keys. 24 bytes for 24-byte TDEA and AES keys, in that case there are no position C and no Vc.

4.2.3 PosB: Position for key version B

16 bytes for 16-byte TDEA or AES key and also for MIFARE keys. 24 bytes for 24-byte TDEA and AES keys, in that case there are no position C and no Vc.

4.2.4 PosC: Position for key version C

16 bytes for 16-byte TDEA or AES key and also for MIFARE keys. If the entry stores 24-byte key, key position C is not available and there is no Vc.

Each position (A, B or C) is configured like the following figure for MIFARE keys.

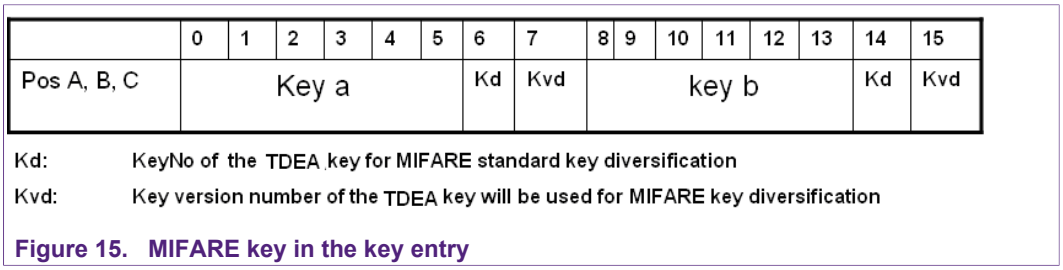

Figure 15. MIFARE key in the key entry

Altogether a MIFARE SAM AV3 can store the following numbers of symmetric keys:

Table 1. Maximum number of keys can be stored in MIFARE SAM AV3

Key	Key Length	Maximum number of keys can be stored in the SAM	Remarks
TDEA	16-byte	128 x 3 = 384	Please do not change the key entry 0 (SAM master key) to MIFARE key. If it is done, purpose of Master key will be void
TDEA	24-byte	128 x 2 = 256	
AES	16-byte	128 x 3 = 384	
AES	24-byte	128 x 2 = 256	
AES	32-byte	128 x 1 = 128	
MIFARE	6-byte	127 x 6 = 762	

Of course, it is possible to mix the key types for MIFARE SAM AV3, e.g. some table entries can contain TDEA keys, some can be AES, and some can be MIFARE keys and so on. But one single table entry can store only one single type of key.

Remark: The keys stored in entry 0 are SAM master key.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

4.2.5 DF_AID: Corresponding DESFire Application ID

This field can (optionally) hold the DESFire AID that is linked to this key entry. If this AID is selected using "*SAM_SelectApplication"* command, and also the application is selected in the DESFire card, then they are in the same level. And the same DESFire key number as given in "DF_KeyNo" field can be used for authenticating the PICC. Even if the key entry is not a key for DESFire PICC, this DF_AID has to be provided, while updating key entries. (Can be set to any value, better set it to 0 s).

4.2.6 DF_KeyNo: Corresponding DESFire key number

This field is used by the command *SAM_SelectApplication* to build a table of keys that are linked to a DESFire AID. Even if the key entry is not a key for DESFire PICC, this DF_KeyNo has to be provided, while updating key entries. (Can be set to any value, better set it to 0).

4.2.7 KeyNoCEK: KST key no for changing the key Entry

The key entry number, which is to be used for changing this key entry. The value FE means that the change is free. The value FF (or any invalid value) irreversibly locks the entry and the content can no longer be changed using symmetric keys, but may be only using Asymmetric keys.

4.2.8 KeyVCEK: Key version for changing key entry

This field contains the version of the key that must be used for changing the key entry, together with KeyNoCEK.

4.2.9 RefNoKUC: Reference Key Usage Counter linked to this key entry

This field contains the reference number (0x00 to 0x0F) for a counter in the KUC table. The referenced counter value will automatically increase each time a key in this entry is used.

Remark: The value must be set to FF if no KUC is used for this entry.

4.2.10 SET: Configuration setting for the key entry

SET bits (16 bits) are used to define the settings of each key entry individually. The incorrect configuration can result in a security flaw in the system. The default value of SET for the MIFARE SAM AV3 key entry is 0000.

Table 2. SET, key entry configuration settings

Bit	Name	Value	Description
0	Session Key dump	0	Will not allow dumping (reading out) the session key.
		1	Will allow dumping the PICC's session keys.
1	RFU	0	Set to 0.
2	Keep IV	0	Init Vector (IV) is always "00".

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

Bit	Name	Value	Description
		1	• After finishing a cryptographic command the updated init vector will be kept for usages in the next cryptographic calculation, if the key is used for PICC like DESFire EV1 standard TDEA and AES mode. • This bit set has no influence for Host key, Offline change key and Offline crypto key class, but only for PICC keys (MIFARE DESFire EV1).
3 - 5	Key type	000	16-byte TDEA DESFire key. The crypto is calculated according to DESFire native TDEA mode if used for DESFire authentication. CRC16 or 4-byte MAC is used wherever necessary.
		001	16-byte TDEA key. The crypto is calculated according to ISO/IEC 10116. In this key type, CRC16 or 4-byte MAC is used wherever necessary.
		010	MIFARE product key. It can be used for the authentication of a MIFARE PICC. This particular key entry can no longer be used for Host and DESFire PICC authentication.
		011	24-byte TDEA key. The crypto is calculated according to ISO/IEC 10116. In this key type, CRC32 or 8-byte CMAC is used wherever necessary.
		100	16-byte AES key. The crypto is calculated according to standard ISO/IEC 10116. In this key type, CRC32 or 8-byte CMAC is used wherever necessary.
		101	24-byte AES key. The crypto is calculated according to standard ISO/IEC 10116. In this key type, CRC32 or 8-byte CMAC is used wherever necessary.
		110	16-byte TDEA Key. The crypto is calculated according to standard ISO/IEC 10116. In this key type, CRC32 or 8-byte MAC is used wherever necessary.
		111	32-byte AES key. The crypto is calculated according to standard ISO/IEC 10116. In this key type, CRC32 or 8-byte CMAC is used wherever necessary.
6-7	RFU	00	Set these bits to 0
8	Host AuthKey	0	Usual security in the host communication
		1	If this bit is set for the SAM master key entry (nr. 0), then host authentication is required for usages of the key entries for secure operations (SAM General Command sets) in each logical channel. For non SAM Master Keys (other key entries), it indicates whether the key can be used for SAM_AuthenticateHost.
9	Disable key entry	0	The key entry is enabled.
		1	The key entry is disabled, can be reactivated by SAM_ChangeKeyEntry command.
10	SAM Lock	0	
		1	If this bit is set for a key entry, then that key can be used for SAM_LockUnlock command. If this bit is set for SAM Master key entry, then SAM_LockUnlock command is a must after SAM reset. For other key entries, it is making that key of “Host key” class type.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

Bit	Name	Value	Description
11 - 15	Disable Feature		Setting of this bit can disable specific features. See detail in [1].

4.2.11 ExtSET: Extended configuration setting for the key entry

Table 3. ExtSET, key entry extended configuration settings

Bit	Name	Value	Description
0	Key class	000	Host key, can be used only for Host authentication. This key entry can be of AES-128 or AES-192.
1		001	PICC key, can be used for PICCs.
2		010	Offline change key. Can be used for offline preparation of change key entry cryptogram. Can be only AES-128 or AES-192 type.
		100	Offline crypto key. Used for general-purpose cryptographic operations. Can be TDEA or AES type.
		101	Offline Upload Key, used for upload of PL code
		110	Offline Perso Key, used for offline encipherment
3	Dumping secret key	0	Dumping of secret key is not allowed.
		1	Dumping of secret key using SAM_DumpSecretKey is allowed. It is only allowed for key class type of PICC and Offline Crypto.
4	Diversification restriction	0	Diversification is not mandatory, when this key is used.
		1	If this bit is set for a key entry, then diversification is mandatory while using that key. It is only allowed for key class type of PICC and Offline Crypto.
5	Reserved for SAM perso	0	The key entry cannot be injected into another SAM. Including the key entry with SAM_EncipherKeyEntry or PKI_EncipherKeyEntries commands will not succeed and result in an error (default configuration)
		1	The key entry is reserved for personalization and is disabled for any other operations. The key can only be used for inclusion by SAM_EncipherKeyEntry and PKI_EncipherKeyEntries. The values of the change entry key (KeyNoCEK and KeyVerCEK) are ignored
6 to 7	RFU	0	Set to 0.

The combination of the SET and ExtSET bits is given in MIFARE SAM AV3 – Key Management and Personalization application note, document number 1823xx.

4.2.12 Va: Version of the key in position A

8-bit version number of the key (16/24/32-byte) in position A. Any value can be given as the version number while updating the key entry.

4.2.13 Vb: Version of the key in position B

8-bit version number of the key (16/24-byte) in position B. Any value can be given as the version number while updating the key entry.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

4.2.14 Vc: Version of the key in position C

8-bit version number of the key (16-byte) in position C. Any value can be given as the version number while updating the key entry. This is not available for entries with 24-byte key length.

4.2.15 Example: addressing key from the SAM

Key Entry	Pos A	Pos B	Pos C		Va	Vb	Vc
...							
5	xxxxxxxxxxxxxx	yyyyyyyyyyyyyyyy	zzzzzzzzzzzzzzzz		i	j	k
6							
..							

Figure 16. Addressing key from key entry

The key entry number 5 and version number i will refer the key “xxxxxxxxxxxxxxxxx”.

The key entry number 5 and version number j will refer the key “yyyyyyyyyyyyyyyyy”.

The key entry number 5 and version number k will refer the key “zzzzzzzzzzzzzzzzz”.

4.2.16 KeyNoAEK and KeyVerAEK

The two 1-byte fields KeyNoAEK and KeyVerAEK specify the symmetric key entry required to access the key.

The permission to access and use a key entry may be restricted to the knowledge of a certain secret. That is, the SAM may be configured to require an active Host Authentication with a specific key in order to grant usage access to the entry.

4.3 PKI Key Storage

Public Key Infrastructure Keys are stored in separate table for each algorithm.

One can store 2 RSA Key pairs and one additional public Key, 8 ECC Keys and 4 curves, and 24 EMV certificates.

All of those tables have their own configuration settings.

4.4 Last Recently Used table of KST entries

SAM always securely stores a copy of the last eight Key entries in the Last Recently Used (LRU) table. It is much faster to access LRU entries than those stored in KST. For a time-critical application it is recommended to store the “time-critical keys” in the LRU. The entries can be put in the LRU by just accessing them once.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

Table 4. Last Recently Used key table

Position	Content of LRU table	After using KST #9	After using KST #10
0	KST # 14	**KST # 09**	**KST # 10**
1	KST # 07	KST # 14	KST # 09
2	KST # 05	KST # 07	KST # 14
3	**KST # 09**	KST # 05	KST # 07
4	KST # 08	KST # 08	KST # 05
5	KST # 01	KST # 01	KST # 08
6	KST # 03	KST # 03	KST # 01
7	KST # 11	KST # 11	KST # 03

How does SAM retrieve entries from LRU table and KST?

- Every time a KST entry is requested, SAM first checks through the contents of the LRU table.
- When it cannot find the entry in the LRU, SAM instead accesses the KST.

After a KST entry is used SAM copies the content of that entry to the top of the LRU table (position 0). Next time, when the same KST is requested SAM will retrieve it from LRU, significantly decreasing the access-time.

EXAMPLES:

Column 2 of the *Table 6* represents an example of the LRU table register. It is a set of the last eight KST entries that were recently used by SAM.

If the requested KST entry is already in the LRU table:

When that happens, SAM will use the entry and move the entry to the top of the table. In the example *Table 6* – SAM looks for KST #9. It locates it on position 3 in the LRU table. This entry is then moved to position 0 of the LRU table – column 3 *Table 6*.

If the requested KST entry is not in the LRU table:

Since SAM is unable to find the entry in LRU table, it looks for the entry in KST. Having located the entry in KST, it copies it to the zero position in the LRU table. The third column of the example *Table 6* represents this particular procedure.

The KST # 10 entry is located by SAM and then copied to the zero position in the LRU table.

4.5 Key Usage Counter (KUC)

The Key-Usage Counter (KUC) table contains 16 entries. One entry of the KUC can be linked to one or more entries in the KST. The KUC entries are automatically incremented every time their corresponding KST keys are used for authentication.

The KUC offers a “usage limiting” capability; a usage limit can be set for every KUC entry. As a result, it restricts the number of times the corresponding keys in KST table can be used for authentication.

The KUC table contains 16 counters and limits.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

Table 5. Key Usage Counter Table

RefNoKUC	Limit	KeyNoCKUC	KeyVCKUC	CurVal
0				
1				
~	~	~	~	~
14				
15				

Description of KUC operation:

- A given KUC is linked to one or more entries in the KST.
- KUC is incremented every time the corresponding KST entry is accessed for authentication.
- When KUC reaches the value defined in the 'Limit' field, the authentication command of a linked KST entry fails, returning ERROR [SW in 1]. The "Limit" field can therefore be used to set limits for the usage of the keys in the KST.

Remark: If the Authentication command fails because of wrong keys, the KUC will also be incremented.

4.5.1 RefNoKUC; Ref nr of Key Usage Counter

The KUC ref. number, ranging from 0 to 15, is used to address an entry of the KUC.

4.5.2 Limit

This field stores the limit for the counter in this KUC entry. 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.

Remark: the initial value for the limit is 0xFFFFFFFF.

4.5.3 KeyNoCKUC; sKST entry nr. of Change KUC entry

The key entry number has to be used for authentication before changing the KUC entry. The addressed key entry must be "Host" or "Offline Change key" class type.

The value 0xFE voids the need for authentication to change the content of this KUC entry.

The value 0xFF irreversibly locks the KUC entry entirely and the content can no longer be modified.

4.5.4 KeyVCKUC; Key Version nr. Change KUC entry

This field contains the version number of the key addressed in KeyNoCKUC that must be used for changing KUC entry.

4.5.5 CurVal; Current Value

This field contains the current value of the KUC.

It is incremented every time the appropriate key from KST (linked to this KUC) is used for authentication.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

Incrementing does **NOT** depend on the result of the authentication. The current value will be incremented even if the authentication fails because of the wrong key being used.

Remark: The Current Value CANNOT be changed.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

5 References

1. **Functional Specification –** Functional Specification of MIFARE SAM AV3, doc nr. 3235xx.
2. **The I2C Specification and User Manual –** UM 10204, http://www.nxp.com/documents/user_manual/UM10204.pdf.
3. **Application note - AN12695 - MIFARE SAM AV3 Quick Start Up Guide**, document number 5210xx, https://www.nxp.com/docs/en/application-note/AN12695.pdf.
4. **Application note - AN12704 - MIFARE SAM AV3 – Host Communication**, document number 5213xx, https://www.nxp.com/docs/en/application-note/AN12704.pdf.

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

6 Legal information

6.1 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.

6.2 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.

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.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer. In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages. Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

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

6.3 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.

6.4 Trademarks

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

MIFARE — is a trademark of NXP B.V.

DESFire — is a trademark of NXP B.V.

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

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

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

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

Tables

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

Figures

All information provided in this document is subject to legal disclaimers.

© NXP B.V. 2020. All rights reserved.

Contents

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

© NXP B.V. 2020. **All rights reserved.**

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

Date of release: 9 January 2020
Document identifier: AN12701
Document number: 521111