AN12694

MIFARE SAM AV3 – For MIFARE Ultralight AES, MIFARE Ultralight C and MIFARE Ultralight EV1

Rev. 1.4 — 28 February 2022

Application note
COMPANY PUBLIC

Document information

Information	Content
Keywords	MIFARE SAM AV3, MF4SAM3, TDEA, AES, RSA, ECC, LRP, MIFARE Ultralight C, MIFARE Ultralight AES
Abstract	This application note presents some examples of using MIFARE SAM AV3 for MIFARE Ultralight C, MIFARE Ultralight AES and MIFARE Ultralight EV1 in non-X interface.

Revision history

Revision history

Rev	Date	Description
1.4	20220228	Security status changed to "Company public"
1.3	20211202	MIFARE Ultralight AES added
1.2	20200108	AN number changed, security status changed into “Company Public”
1.1	20190923	Added example for MIFARE Ultralight EV1
1.0	20190423	Initial version

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 presents examples of using MIFARE SAM AV3 (referred to SAM in this document, if not otherwise mentioned) for MIFARE Ultralight C. In this document, the SAM is used in S mode (X mode is described in doc nr. 5219xx) 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 [4]

This application note is a supplement document for application development using MIFARE SAM AV3. Should there be any confusion please check MIFARE SAM AV3 data sheet [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 data sheets, datasheets, application notes or design guides.

1.2 Abbreviation

Refer to Application note “MIFARE SAM AV3 – Quick Start up Guide” [4].

1.3 Examples presented in this document

The following symbols have been used to mention the operations in the examples:

= Preparation of data by SAM, PICC or host.

> Data sent by the host to SAM or PICC (if not mentioned, SAM).

< Data Response from SAM or PICC (if not mentioned, SAM).

C-APDU:

CLA	INS	P1	P2	Lc	Data (nc)	Le

R-APDU:

Response data	SW1	SW2

Please note, that the numerical data are used solely as examples. They appear in the text in order to clarify the commands and command data.

Any data, values, cryptograms are expressed as hex string format if not otherwise mentioned e.g. 0x563412 in hex string format represented as “123456”. Byte [0] = 0x12, Byte [1] = 0x34, Byte [2] = 0x56.

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

1.4 S interface

The host is managing the communication to SAM and MIFARE Ultralight C.

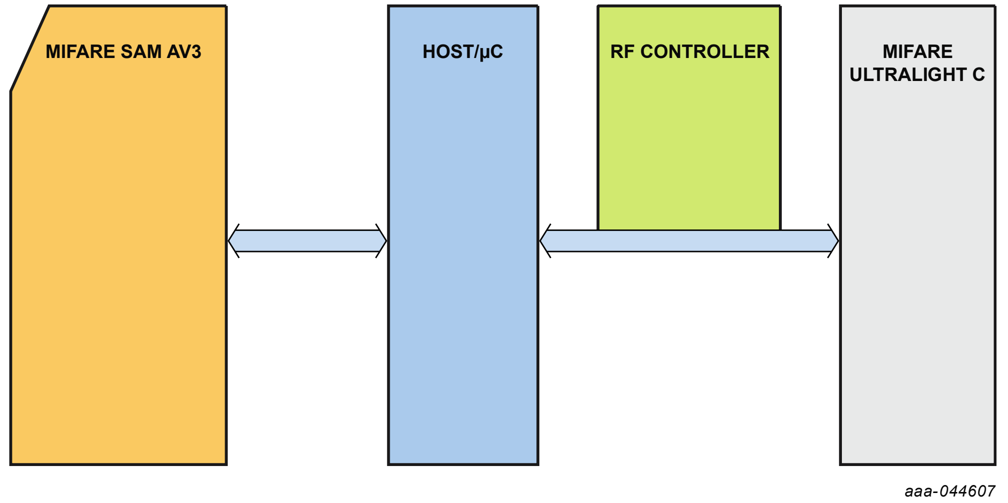


Figure 1. Architecture in S interface with “Ultralight C”

2 Using MIFARE SAM AV3 for MIFARE Ultralight C

MIFARE SAM AV3 can be used to store the MIFARE Ultralight C key, and the stored key can be used for authentication of MIFARE Ultralight C.

2.1 Downloading the MIFARE Ultralight C key into SAM from Host

Downloading of different keys to SAM is explained in [5]. The SAM key entry settings are different for different types of crypto and PICCs. The incorrect setting will result to authentication error. The right SAM key entry settings for MIFARE Ultralight C key are shown in the following table:

Table 1. SAM Key Entry setting for MIFARE Ultralight C Key

SAM Key entry setting	Accreditation[1] SAM key entry setting for MIFARE Ultralight C Key	Validation[2] SAM key entry setting for MIFARE Ultralight C Key
SAM Key entry “SET” bits		
b0: Allow dumping session key.	‘0’	‘0’
b1: RFU must be set to 0.	‘0’	‘0’
b2: Keep IV	‘1’	‘1’
b5b4b3: Key type	TDEA ISO 10116 (16-bit CRC, 4-byte MAC) ‘0001’	TDEA ISO 10116 (16-bit CRC, 4-byte MAC) ‘0001’
b7b6: RFU must be set to 0	‘00’	‘00’
b8: Host Auth Key for unlocking the LC	‘0’	‘0’
b9: Disable key entry	‘0’	‘0’
b10: Lock Key	‘0’	‘0’
b11: Disable SAM_ChangeKeyPICC	‘0’	‘0’
b15b14b13b12	‘0000’	‘0000’
So the SET =	“0C00” (in hex string LSB MSB)	“0C00” (in hex string LSB MSB)
SAM Key entry “ExtSET” bits		
b2b1b0: Key class	‘001’	‘001’
b3: Allow dumping secret key.	‘1’	‘0’
b4: Restricted for diversification. Strongly recommended to use.	‘1’	‘1’
b15b14b13b12b11b10b9b8b7b6b5	'00000000000'	'00000000000'

[1] The SAMs used in the card personalization/ issuing machines. The key is downloaded from this SAM to MIFARE Ultralight C.
[2] The SAMs used in Check-in/out terminals.

2.2 Downloading key to MIFARE Ultralight C from SAM

In this example key entry number 4 will be used, which has the following setting:

SET = 0C00

DO NOT allow dump Session key

Keep IV

Key type: TDEA ISO 10116 (16-bit CRC, 4-byte MAC)

ExtSET = 1900

PICC key

Allow dumping secret key [2]

Diversification is mandatory

Table 2. Loading MIFARE Ultralight C Key from SAM

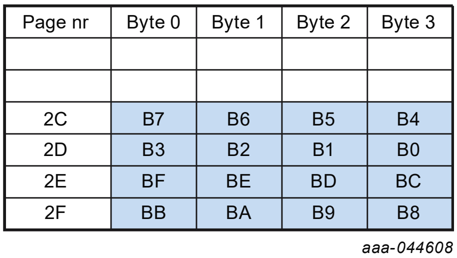
step	Indication		Data / Message	Comment
	MIFARE SAM needs to unlock (recommended to lock the SAM) using SAM_AuthenticateHost command			
1	SAM_DumpSecretKey C-APDU	>	80D602000904B0044DC5E1ED258000	P1=02; use key diversification. Data field = SAM key entry nr, version number and DivInp (044DC5E1ED2580, the UID)
2	SAM_DumpSecretKey R-APDU	<	9B5E1BB7D44676104F586D99F0C07E569000	Diversified key and SW1SW2
3	Write this key to MIFARE Ultralight C	=	Key = 9B5E1BB7D44676104F586D99F0C07E56; Write ‘107646D4’ to page 2C Write ‘B71B5E9B’ to page 2D Write ‘567EC0F0’ to page 2E Write ‘996D584F’ to page 2F	Key storage in MIFARE Ultralight C is shown in § 2.2.1.

2.2.1 Storage of TDES key in MIFARE Ultralight C

In MIFARE Ultralight C, the key bytes are stored in a different order. The following example will make it clear.

Key = B0B1B2B3B4B5B6B7B8B9BABBBCBDBEBF

This key stored in the MIFARE Ultralight C memory as shown in figure 2.



Page nr	Byte 0	Byte 1	Byte 2	Byte 3
2C	B7	B6	B5	B4
2D	B3	B2	B1	B0
2E	BF	BE	BD	BC
2F	BB	BA	B9	B8

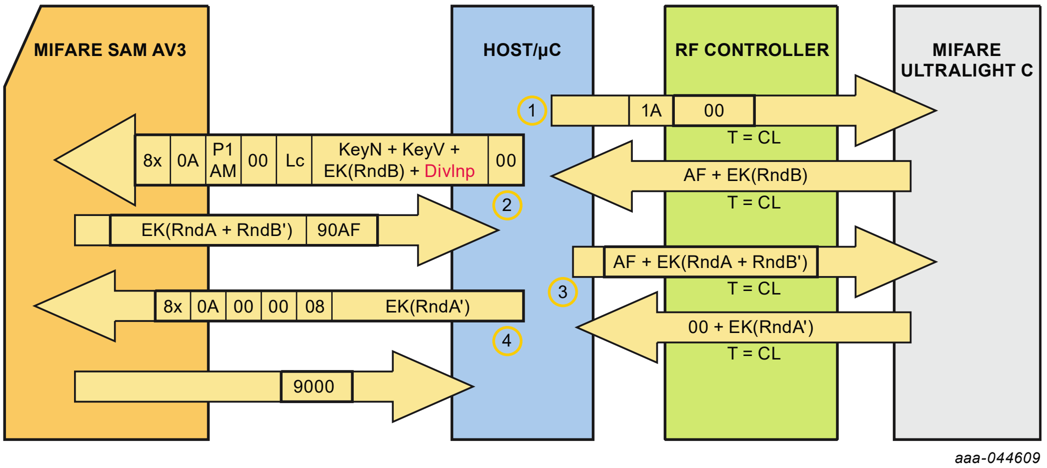
aaa-044608

Figure 2. Storage of TDES key in MIFARE Ultralight C

2.3 Authenticating MIFARE Ultralight C using the SAM

The full authentication is managed by host microcontroller.

[2] Only recommended to use for the SAMs in personalization/issuing machines.



1. Host/uC sends the authentication command to MIFARE Ultralight C, MIFARE Ultralight C returns the challenge.
2. Host/uC sends the challenge to the SAM. SAM prepares the response of the MIFARE Ultralight C challenge and generates its own challenge.
3. Host/uC sends the response of SAM to MIFARE Ultralight C. MIFARE Ultralight C returns the response of the SAM challenge.
4. Host/uC sends the MIFARE Ultralight C response to the SAM for verification. SAM checks it and finally returns the status of the authentication.

Figure 3. MIFARE Ultralight C Authentication using SAM

2.3.1 MIFARE Ultralight C Authentication with diversified key

In this example key entry number 4 and version B0 will be used, which has the following setting:

SET = 0C00

DO NOT allow dump Session key

Keep IV

Key type: TDEA ISO 10116 (16-bit CRC, 4-byte MAC)

ExtSET = 11

PICC key

Diversification is mandatory

In this example, the Key Version “B0” is used for authentication.

Table 3. MIFARE Ultralight C Authentication with diversified key

step	Indication		Data / Message	Comment
1	Send authentication command to MIFARE Ultralight C	>	1A00	Authentication cmd 1A and key number 00 (always fixed).
2	Challenge from MIFARE Ultralight C	<	AF5876F623666D64C0	AF is the status byte and 8-byte Ek(RndB).

Table 3. MIFARE Ultralight C Authentication with diversified key*...continued*

step	Indication		Data / Message	Comment
3	First part of the SAM_ AuthenticatePICC command	>	800A11001104B05876F623666D64 C0044DC5E1ED258000	P1 = 11; CMAC based key diversification, key selection must be made by key entry number (always). Data field is SAM key entry number, version number, Ek(RndB received in step 2) and DivInp (UID = 044DC5E1ED2580).
4	Answer of the SAM	<	C4B3B7D5729EE6CAD968442C07 6EBCD790AF	Ek(RndA+RndB´) and status byte 90AF.
5	Answer of the SAM is sent to MIFARE Ultralight C	>	AFC4B3B7D5729EE6CAD968442C 076EBCD7	AF is the cmd and Ek(RndA+RndB´).
6	Response of the MIFARE Ultralight C	<	00CE1885E89769B284	00 is the status, i.e. authentication is successful and Ek(RndA´).
7	Second part of the SAM_ AuthenticatePICC command	>	800A000008CE1885E89769B284	Ek(RndA´) is sent to the SAM
8	Answer of the SAM	<	9000	SAM decides whether the MIFARE Ultralight C response is correct or not.

2.3.2 MIFARE Ultralight C Authentication with non diversified key

In this example key entry number 7 will be used, which has the following setting:

SET = 0C00

DO NOT allow dump Session key

DO NOT allow crypto with secret key

Keep IV

Key type: TDEA ISO 10116 (16-bit CRC, 4-byte MAC)

ExtSET = 0100

PICC key.

In this example, we use the Key Version “01” for authentication.

Table 4. MIFARE Ultralight C Authentication with non diversified key

step	Indication		Data / Message	Comment
1	Send authentication command to MIFARE Ultralight C	>	1A00	Authentication cmd 1A and key number 00 (always fixed).
2	Challenge from MIFARE Ultralight C	<	AFAE88277CD976C4C1	AF is the status byte and 8-byte Ek(RndB).
3	First part of the SAM_ AuthenticatePICC command	>	800A00000A0701AE88277CD976C 4C100	P1 = 00; no key diversification, key selection must be made by key entry number (always). Data field is SAM key entry number, version number and Ek(RndB received in step 2).
4	Answer of the SAM	<	E1C71B64CEE3397FEAE3DE35C D1D581790AF	Ek(RndA+RndB´) and status byte 90AF.

Table 4. MIFARE Ultralight C Authentication with non diversified key*...continued*

step	Indication		Data / Message	Comment
5	Answer of the SAM is sent to MIFARE Ultralight C	>	AFE1C71B64CEE3397FEAE3DE35 CD1D5817	AF is the cmd and Ek(RndA+RndB´).
6	Response of the MIFARE Ultralight C	<	00B3E918D76F63545D	00 is the status, i.e. authentication is successful and Ek(RndA´).
7	Second part of the SAM_ AuthenticatePICC command	>	800A000008B3E918D76F63545D	Ek(RndA´) is sent to the SAM
8	Answer of the SAM	<	9000	SAM decides whether the MIFARE Ultralight C response is correct or not.

3 Using MIFARE SAM AV3 with MIFARE Ultralight EV1

MIFARE SAM AV3 also supports the password authentication used in MIFARE Ultralight EV1. The password in this case is not stored as such in the SAM, but it is generated out of an AES128 PICC Key using a CMAC-based key diversification algorithm. The algorithm itself is the same as the default MIFARE key diversification algorithm, except for the diversification constant, which is 0x02 in this case.

3.1 MIFARE Ultralight EV1 password derivation example

Master key (K) = 00000000000000000000000000000000, which will be diversified.

Table 5. Example – Password derivation

step	Indication		Data/ Message	Comment
CMAC sub key generation				
1	Master key (K)	=	00000000000000000000000000000000	The key, which is going to be diversified
2	K0	=	66E94BD4EF8A2C3B884CFA59CA342B2E	CIPHK(0b), AES (K, 16-byte 0s).
3	K1	=	CDD297A9DF1458771099F4B39468565C	The first sub key, see in [CMAC].
4	K2	=	9BA52F53BE28B0EE2133E96728D0AC3F	The second sub key, see in [CMAC].
Password generation				
5	Diversification input (M)	=	empty	DIn this example, no diversification input is used. for diversified passwords, the UID or other unique inpoputs can be used.
6	Add the Div Constant at the beginning of M	=	02	Constant || M , constant is fixed, must be 0x02. M is empty in this example.
7	Do I need Padding	=	Yes	The algorithm always needs 32-byte block for AES; so far we have 1 bytes (step 6).
8	Padding	=	80000000000000000000000000000000000000000000000000000000000000	31-byte padding to make 32-byte block.
9	CMAC input D	=	0280000000000000000000000000000000000000000000000000000000000000	32 bytes (step 6
10	Last 16-byte is XORed with K2	=	02800000000000000000000000000000000000009BA52F53BE28B0EE2133E96728D0AC3F	As the padding is added the last block is XORed with K2, if padding is not added, then XORed with K1.
11	Encryption using K	=	9F83B2832485C2EFD24520634A952C397664D536FCA3EA1C2393D90B35DC44A0	Standard AES encryption with IV = 00s in CBC mode
12	Diversified password vector (PV)	=	7664D536FCA3EA1C2393D90B35DC44A0	Last 16-byte block. (CMAC)
13	Password	=	7664D536	PV[0:3]
14	PACK	=	44A0	PV[14:15]

The command sequence for the passwort authentication with a MIFARE Ultralight EV1 is rather simple.

The following example showes a password authentication with an all 00's AES128 PICC key stored in KeyEntry 0x02. The derived key according to Table 5 is already stored in the MIFARE Ultralight EV1 tag.

Table 6. Password Authentication with MIFARE Ultralight EV1

step	Indication		Data/ Message	Comment
1	Send SAM_PwdAuthUL	>	800B000002020000	KeyEntry 0x02, version 0x00
2	Receive derived password	<	7664D53690AF	The SAM AV3 answers with the derived password according the derivation algorithm.
3	Send PWD_Auth to MIFARE Ultralight EV1	>	1B7664D536	PWD_Auth command to MIFARE Ultraligt EV1
4	Receive PACK from MIFARE Ultralight EV1	<	44A0	If the password is correct, MIFARE Ultralight EV1 answers with PACK
5	Send PACK to SAM AV3	>	800B00000244A0	PACK is provided to the SAM AV3 in the second step of the SAM_PwdAuthUL command
6	Successful authentication	<	9000	Successful authentication with the MIFARE Ultralight EV1

4 Using MIFARE SAM AV3 with MIFARE Ultralight AES

MIFARE SAM AV3 fully supports all crypto operations necessary for MIFARE Ultralight AES, even though there are no native SAM commands for MIFARE Ultralight AES available. Therefore, to use MIFARE Ultralight AES with MIFARE SAM AV3, an OfflineCrypto key and one RAM key entry is needed.

4.1 Creating a SAM key entry for usage with MIFARE Ultralight AES

To support the CMAC-based secure messaging from MIFARE Ultralight AES, the secret key to be used needs to be injected into the SAM AV3 symmetric keystore. This key can be used either diversified or non-diversified. The session key that is generated during the 3-pass mutual authentication is stored then in one of the 4 available RAM key entries.

MIFARE Ultralight AES needs an AES-128 key of key class "OfflineCrypto". **Note:** A key of key class "PICC" will not work, as the secure messaging used in MIFARE Ultralight AES is not natively implemented in MIFARE SAM AV3.

Table 7. Preparing the KeyEntries for use with MIFARE Ultralight AES

Step	Command	Direction	Message	Comment
1	SAM_ ChangeKeyEntry	>	80C101FF40000000000000000000000 0000000000000000000000000000000 0000000000000000000000000000000 0000000000000000000000000FF2000 0000000400FEFE	Inject an AES128 all 00s (default key) key into SAM KeyEntry 0x00. KeyClass is OfflineCrypto Key
2	Response	<	9000	Success
3	SAM_ ChangeKeyEntry	>	80C1E08F40000000000000000000000 0000000000000000000000000000000 0000000000000000000000000000000 0000000000000000000000000FF2000 0000000400FEFE	Prepare the RAM KeyEntry 0xE0 for the use with the SAM_DeriveKey command. The settings of the RAM key need to be the same as for the source key before using the SAM_DeriveKey command, to ensure that the derived key (session key in this case) cannot be used in a different way than the source key.
4	Response	<	9000	Success

4.2 Authenticating MIFARE Ultralight AES

There is no dedicated command for Authenticating MIFARE Ultralight AES available. The authentication could be done with with SAM_AuthenticatePICC command as well, but as the secure messaging used by MIFARE Ultralight AES is not implemented in MIFARE SAM AV3, the session keys would need to be dumped out of the SAM. Therefore, the below shown approach is the better option, as no key ever leaves the MIFARE SAM AV3.

Table 8. Authenticating MIFARE Ultralight AES

Step	Command	Direction	Message	Comment
1	ActivateOffline Key	>	80010000020100	Activate the secret key
2	Response	<	9000	success
3	Authenticate part 1	>	1A00	First Part of Authenticate command sent to MIFARE Ultralight AES

Table 8. Authenticating MIFARE Ultralight AES*...continued*

Step	Command	Direction	Message	Comment
4	E(Kx,RndB)	<	AF37B7F49CD707F8D8E29DDEC256912187	0xAF + E(Kx,RndB)
5	LoadIV	>	807100001000000000000000000000000000000000	Sets the SAM's IV to all 0x00s
6	Response	<	9000	success
7	SAM_ DecipherOffline_Data	>	800D00001037B7F49CD707F8D8E29DDEC25691218700	Decrypts the encrypted RndB
8	RndB	<	D220B067DE955EFA0A24623F4F216AC59000	RndB
9	GetRandom	>	8084000010	Generates 16 byte random data as RndA
10	RndA	<	07F8AAE1B62FB3930977BDCD16157E8B9000	RndA
11	LoadIV	>	807100001000000000000000000000000000000000	Sets the SAM's IV to all 0x00s
12	Response	<	9000	success
13	SAM_ EncipherOffline_Data	>	800E00002007F8AAE1B62FB3930977BDCD16157E8B20B067DE955EFA0A24623F4F216AC5D200	Encrypts the concatenation of RndA and RndB' (RndB' is the rotation of RndB by one byte)
14	E(Kx,RndA||RndB')	<	66FDB31BFD79F3C02E17C44FCDB7466B669DFA2F986F568725703DDF47D0243D9000	Encrypted RndA || RndB'
15	Authenticate part 2	>	AF66FDB31BFD79F3C02E17C44FCDB7466B669DFA2F986F568725703DDF47D0243D	Authenticate part 2 sent to MIFARE Ultralight AES
16	E(Kx,RndA')	<	002D9194C800DBA0C4B8A85CACD54F6568	0x00 (success) and encrypted RndA'
17	LoadIV	>	807100001000000000000000000000000000000000	Sets the SAM's IV to all 0x00s
18	Response	<	9000	success
19	SAM_ DecipherOffline_Data	>	800D0000102D9194C800DBA0C4B8A85CACD54F656800	Decrypts the encrypted RndA'
20	RndA'	<	F8AAE1B62FB3930977BDCD16157E8B079000	RndA'
25	SAM_DeriveKey	>	80D70000230100E05AA50001008007F878C106486D065EFA0A24623F4F216AC50977BDCD16157E8B	Generates the session key and stores it in the prepared RAM key entry. The RAM key entry needs to have the same settings as the source key before using this command. The data field contains the source KeyNo. and Version (0100), the RAM KeyNo. (E0) and the session vector (5Ah||A5h||00h||01h||00h||80h||RndA[15..14]|| RndA[13..8] XOR RndB[15..10])|| RndB[9..0]||RndA[7..0])
26	Response	<	9000	success

4.3 CMAC communication example

The following example shows a basic command exchange with MIFARE Ultralight AES using secure messaging. The key used is the session key generated in Table 8.

Note: For CMAC verification after upon reception of a response from the MIFARE Ultralight AES, either the SAM_GenerateMAC command (as used in the example), or the SAM_VerifyMAC command can be used, with the input and MAC as payload.

Table 9. Secure messaging example

Step	Command	Direction	Message	comment
GetVersion				
1	SAM_ ActivateOfflineKey	>	8001000002E000	SAM_ActivateOfflineKey 0xE0 (previously derived key in RAM keystore)
2	Success	<	9000	
3	SAM_LoadInitVerctor	>	807100001000000000000000000000000000000000	SAM_LoadInitVerctor to 00s
4	Success	<	9000	
5	SAM_GenerateMAC	>	807C00800300006000	SAM_GenerateMAC, input is the CmdCtr (0000h) and the command code 60h
6	Response	<	F010B877942B07909000	returned 8 byte CMAC and success code
7	GetVersion	>	60F010B877942B0790	Send GetVersion command + MAC to MIFARE Ultralight AES
8	Version Info	<	0004030104000F03F6D458CD5C136825	Response: Version Info + CMAC
9	SAM_LoadInitVerctor	>	807100001000000000000000000000000000000000	SAM_LoadIV to 00s
10	Success	<	9000	
11	SAM_GenerateMAC	>	807C00800A01000004030104000F0300	SAM_GenerateMAC, input is the increased CmdCtr (0001h as LSB first) and the command response (status code + version info)
12	Response	<	F6D458CD5C1368259000	returned 8 byte CMAC and success code
13	Compare	=		compare CMACs
Read page 12h				
14	SAM_LoadInitVerctor	>	807100001000000000000000000000000000000000	SAM_LoadIV to 00s
15	Success	<	9000	
16	SAM_GenerateMAC	>	807C0080040200301200	SAM_GenerateMAC, input is the CmdCtr (0002h as LSB first), command code (30h) and payload (page address 12h)
17	Response	<	5EA44B21D7F660269000	returned 8 byte CMAC and success code

Table 9. Secure messaging example ***...continued***

Step	Command	Direction	Message	comment
18	READ page 12h	>	30125EA44B21D7F66026	READ command and CMAC sent to MIFARE Ultralight AES
19	Data in pages 12h-15h	<	0000000000000000000000000000000 05B536EAB0D03CB8C	returned data and 8 byte CMAC
20	SAM_LoadInitVerctor	>	8071000010000000000000000000000 00000000000	SAM_LoadIV to 00s
21	Success	<	9000	
22	SAM_GenerateMAC	>	8070080120300000000000000000000 00000000000000000	SAM_GenerateCMAC, input is the command code and the response data
23	Response	<	5B536EAB0D03CB8C9000	returned 8 byte CMAC and success code
24	Compare	=		compare MACs

4.4 Downloading a key from MIFARE SAM AV3 to MIFARE Ultralight AES

As the MIFARE Ultralight AES does not support a secure mechanism for key injection, this process needs to be done in a secure environment, as the key is handled in plain. If a key stored inside a MIFARE SAM AV3 needs to be injected into a MIFARE Ultralight AES, the key needs to be dumped from the SAM and written into the corresponding memory area in MIFARE Ultralight AES.

To be able to dump a secret key from MIFARE SAM AV3, the KeyEntry needs to have bit 3 oft the ExtSET enabled. This will make the secret key exportable in plain or encrypted form, using the SAM_DumpSecretKey command. Additionally, in case the key should be used in diversified form, the bit 4 of ExtSET should also be set, to only allow dumping if a diversification input is provided.

Table 10. Secure messaging example

Step	Command	Direction	Message	comment
dump plain				
1	SAM_ ChangeKeyEntry	>	80C101FF40000000000000000000000 0000000000000000000000000000000 0000000000000000000000000000000 0000000000000000000000000FF2000 00010209000000	Load Key into KeyEntry 0x01 of MIFARE SAM AV3. ExtSet bit 3 is enabled, dump of secret key is allowed. (ExtSet = 0x0009)
2	Success	<	9000	
3	SAM_ DumpSecretKey	>	80D6000002010000	Dump the secret key in plain
4	Key Data	<	0000000000000000000000000000000 09000	Secret key and status code
dump diversified				
5	SAM_ ChangeKeyEntry	>	80C101FF40000000000000000000000 0000000000000000000000000000000 0000000000000000000000000000000 0000000000000000000000000FF2000 00010219000000	Load Key into KeyEntry 0x01 of MIFARE SAM AV3. ExtSet bit 3 and bit 4 is enabled, dump of secret key is allowed but only in diversified form (ExtSet = 0x0019)
6	Success	<	9000	

Table 10. Secure messaging example *...continued*

Step	Command	Direction	Message	comment
7	SAM_ DumpSecretKey	>	80D6020009010004112233445566 00	Dump the secret key in plain, diversified form (P1 = 0x02), div input = 04112233445566
8	Key Data	<	2360D14689E17C7AA9821665E68A00 999000	Diversified secret key and status code

The dumped key needs to be written inside the AES Key_x area inside the MIFARE Ultralight AES memory. This process is described in the data sheet, as well as in the application note features and hints.

5 References

1. **Data sheet – Data sheet MIFARE SAM AV3**, document number ds3235xx.
2. **User manual – UM5385 MF4SAM3 - System guidance, delivery and operation manual**, document number um5385xx.
3. **Data sheet – MIFARE Ultralight C**, https://www.nxp.com/docs/en/data-sheet/MF0ICU2.pdf
4. **Data sheet - MIFARE Ultralight AES MF0AES(H)20**, document number ds5379xx
5. **Application note - MIFARE Ultralight AES Features and Hints**, document number an7106xx
6. **Application note – AN12695 – MIFARE SAM AV3 – Quick Start up Guide**, https://www.nxp.com/docs/en/application-note/AN12695.pdf.
7. **Application note – AN5212 MIFARE SAM AV3 – Key Management and Personalization**, document number an5212xx.
8. **Application note – AN10922 Symmetric Key Diversifications**, https://www.nxp.com/docs/en/application-note/AN10922.pdf.
9. **CMAC specification**: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf.

6 Legal information

6.1 Definitions

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

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.

Suitability for use in 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.

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, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

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.

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

DESFire — is a trademark of NXP B.V.

MIFARE — is a trademark of NXP B.V.

MIFARE Classic — 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.

Tables

Figures

Contents

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

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

Date of release: 28 February 2022
Document identifier: AN12694