AN12706

MIFARE SAM AV3 - for MIFARE Plus

Rev. 1.2 — 12 May 2020
521412

Application note
COMPANY PUBLIC

Document information

Information	Content
Keywords	MIFARE SAM 3 MF4SAM3, TDEA, AES, RSA, ECC, MIFARE Plus EV1, MIFARE Plus EV2
Abstract	This application note presents some examples of using MIFARE SAM AV3 for MIFARE Plus MIFARE PLUS EV1 and MIFARE Plus EV2

Revision history

Rev	Date	Description
1.2	20200512	MIFARE Plus EV2 included
1.1	20200110	AN number changed, security status changed into “Company Public”.
1.0	20190423	Initial revision

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 Plus S,SE,X, MIFARE Plus EV1 and MIFARE Plus EV2. In this document, the SAM is used in non-X interface (X interface 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.

In the following, all examples are valid for both, MIFARE Plus and MIFARE Plus EV1, except otherwise mentioned.

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

In this document the term „MIFARE Plus card“ refers to a MIFARE Plus IC-based contactless card.

If not otherwise stated, the examples in this document apply for MIFARE Plus S,SE,X, MIFARE Plus EV1 and MIFARE Plus EV2.

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

[1] MIFARE Ultralight C, MIFARE Classic, MIFARE Classic EV1, MIFARE Plus, MIFARE Plus EV1, MIFARE Plus EV2, MIFARE DESFire, MIFARE DESFire EV1, MIFARE DESFire EV2, MIFARE DESFire EV3

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.

1.4 S interface

The host is managing the communication to SAM and MIFARE Plus EV1 card.

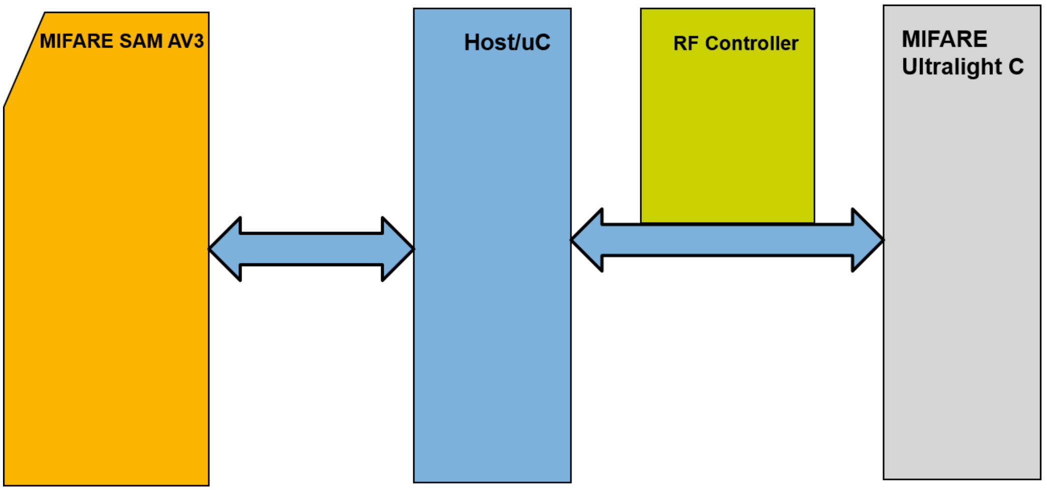

Figure 1. Architecture in non-X interface

2 Using MIFARE SAM AV3 for MIFARE Plus

2.1 SAM Personalization for MIFARE Plus

MIFARE SAM AV3 personalization is described in document number 5212xx [5]. For MIFARE Crypto1, the key type has to be “MIFARE” and for AES, the key type has to be “AES-128” (Do NOT set “Keep IV” option of the setting). The key class has to be defined for PICC keys.

2.2 SAM AV3 with MIFARE Plus in SL0

MIFARE Plus SL0 requires a key to be sent in plain to the MIFARE Plus chip. Therefore, the application should dump the MIFARE Plus keys from the SAM and the setting must allow dumping the secret key. Make sure that these SAMs where dumping secret keys are allowed are only used in the secure environment.

One example SAM configuration scenario is presented in the following:

- Set bit number 10 to 1 in Setting for the SAM Master key entry, which will mandate a unlock after the SAM is powered up.
- Set bit number 3 to 1 in ExtSet for allowing dumping secret key.
- Set bit number 4 to 1 in ExtSet for must key diversification.

The steps for MIFARE Plus personalization in SL0:

- Authenticate host to unlock the SAM, the communication mode can be set to plain communication, because the key sent to MIFARE Plus is anyway plain.
- Dump the secret key by providing the diversification input.
- Send this key to MIFARE Plus using WritePerso command.

2.2.1 Example – MIFARE Plus SL0 personalization using SAM

Secret key (Kx) = 000102030405060708090A0B0C0D0E0F.

Table 1. Example - MIFARE Plus SL0 personalization using SAM

step	Indication		Data / Message	Comment
1	Activate the MIFARE plus card up to ISO/IEC 14443-4.			
2	SAM_AuthenticateHost with Key entry 0 and right version to unlock the SAM, use communication mode plain.			
3	Dump Secret key C-APDU	>	80D60200091001046055A961288000	P1 = 0x02; means Diversification is used. Data field = SAM key entry number, version number and 7-byte MIFARE Plus card UID as diversification input. (Diversification input can be up to 31 bytes). The dumping can be made also encrypted using the secure messaging [8].
4	R-APDU	<	7299CE10F5DCD7B994A59E17B57533729000	The diversified MIFARE Plus key and 2-byte status.

step	Indication		Data / Message	Comment
5	Write perso command to MIFARE Plus card	<	A800907299CE10F5DCD7B 994A59E17B5753372	Cmd = A8; Block number = 0090, then 16-byte key.
6	Response to write perso command	>	90	Successful
7	Follow the steps 3 to 6 with the appropriate values as many times required and finally commit.			
8	Commit perso command to MIFARE Plus card	<	AA	
9	Response to commit perso command	>	90	Successful, the MIFARE Plus card is now in SL1.

Configure the SAM in the right way, that it requires authentication for dumping the key.

2.3 SAM AV3 with MIFARE Plus SL1

MIFARE Plus SL1 (security level 1) is the MIFARE Classic compatible mode. MIFARE Classic related use of SAM is described in [7].

This section is relevant for MIFARE Plus EV0 (X, S, SE), MIFARE Plus EV1 and MIFARE Plus EV2.

2.3.1 Example – Optional AES authentication in MIFARE Plus SL1

In this example MIFARE Plus SL0 AES key is stored in SAM key entry number 5. The key has to be AES-128 type and key class to be PICC key.

Table 2. Example - AES authentication at MIFARE Plus SL1

step	Indication		Data / Message	Comment
1	Activate the MIFARE Plus card up to ISO/IEC 14443-3.			
2	SAM_AuthenticateHost with Key entry 0 and right version to unlock the SAM (if it is required), for simplicity let’s take communication mode plain.			
3	Send following authentication command to MIFARE Plus	>	760490	Cmd = 0x76, SL1 optional AES key is stored in block number 0x9004 of MIFARE Plus. Use ISO/IEC 14443-3 frame, no prologue field.
4	Response of MIFARE Plus	<	9009FEAAF9A70AFFAA 2C2E1004E84CCD21	The status byte 0x90 and 16-byte En (RndB).
5	C-APDU to SAM, 1st part of SAM_AuthenticateMFP command	>	80A3020012050109FEA AF9A70AFFAA2C2E100 4E84CCD2100	Data = SAM key entry nr, version and 16-byte En (RndB). Here diversification is not used, but it is recommended for real application.

step	Indication		Data / Message	Comment
6	R-APDU from SAM	<	10876FFD4F87030A2966F8EC235AAA30747DE0B870C523C25D4A53A5A3B71CCA90AF	32-byte En(RndA+RndB´)+SW1SW2 (90AF)
7	Send 2nd part of authentication command to MIFARE Plus	>	7210876FFD4F87030A2966F8EC235AAA30747DE0B870C523C25D4A53A5A3B71CCA	Cmd = 0x72 and 32-byte En(RndA+RndB´); Use ISO/IEC 14443-3 (no prologue field) frame.
8	Response of MIFARE Plus	<	904D4C03DFB3C5B4129B846D635CDF922C	Status byte 0x90(success) and Ek(RndA´).
9	C-APDU to SAM, 2nd part of SAM_AuthenticateMFP command	>	80A30000104D4C03DFB3C5B4129B846D635CDF922C00	Data = Ek(RndA´). Put here Le = 0x00 although no data in response.
10	R-APDU from SAM	<	9000	SW1SW2 = 9000, authentication is successful.

The optional AES authentication can really provide you considerable security while using MIFARE Plus in MIFARE Classic mode.

2.3.2 Example – Switch to Security Level 3

In this example MIFARE Plus SL3 switch key is stored in SAM key entry number 5. The key has to be AES-128 type and key class to be PICC key.

For MIFARE Plus EV0 (X, S, SE), it is mandatory to switch to SL2 before switching to SL3. This works in the same way as described below, the only difference is, that the Block to be authenticated with must be 0x9002.

Table 3. Example - Switching to SL3

step	Indication		Data / Message	Comment
1	Activate the MIFARE Plus card up to ISO/IEC 14443-4. Although the SAK at MIFARE Plus SL1/SL2 does not mention it supports ISO/IEC 14443-4, it does.			
2	SAM_AuthenticateHost with Key entry 0 and right version to unlock the SAM (if it is required), for simplicity let's take communication mode plain.			
3	Send following authentication command to MIFARE Plus	>	760390	Cmd = 0x76, SL3 switch key is stored in block number 0x9003 of MIFARE Plus. Use ISO/IEC 14443-4 (T=CL) frame.
4	Response of MIFARE Plus	<	90301A48F04A433BFD6ECD07F5D5ADA33B	The status byte 0x90 and 16-byte En (RndB).
5	C-APDU to SAM, 1st part of SAM_AuthenticateMFP command	>	80A30F00120511301A48F04A433BFD6ECD07F5D5ADA33B00	Data = SAM key entry nr, version and 16-byte En (RndB). Here diversification is not used, but it is recommended for real application.
6	R-APDU from SAM	<	56B865122809158E61E408A90B6FDF37698F32640C822F0FA28023412162C2C090AF	32-byte En(RndA+RndB´)+SW1SW2 (90AF)

step	Indication		Data / Message	Comment
7	Send 2nd part of authentication command to MIFARE Plus	>	7256B865122809158E61E408A90B6FDF37698F32640C822F0FA28023412162C2C0	Cmd = 0x72 and 32-byte En(RndA+RndB´); Use ISO/IEC 14443-4 (T=CL) frame.
8	Response of MIFARE Plus	<	90D4CD9501C4BC8A92AD148F4E31C6A0CE	Status byte 0x90(success) and Ek(RndA´).
9	C-APDU to SAM, 2nd part of SAM_AuthenticateMFP command	>	80A3000010D4CD9501C4BC8A92AD148F4E31C6A0CE00	Data = Ek(RndA´). Put here Le = 0x00 although no data in response.
10	R-APDU from SAM	<	9000	SW1SW2 = 9000, authentication is successful. The MIFARE Plus card is switched to Security level 3 (SL3).

In this example the following authentication of MIFARE Plus command has been used. The first authentication command can be used as well.

As no PCDCap2.1 is present, EV0 backwards compatible secure messaging is used in above example.

2.4 SAM AV3 with MIFARE Plus SL3

All the functions supported by MIFARE Plus in SL3 are supported by MIFARE SAM AV3. Some examples are shown in the following sections.

This section is relevant for, MIFARE Plus EV0 (X, S, SE), MIFARE Plus EV1 and MIFARE Plus EV2. Secure Messaging for MIFARE Pus S,SE,X is used. For specific MIFARE Plus EV1 examples see next section.

2.4.1 Example – MIFARE Plus SL3 First Authentication

In this example MIFARE Plus AES key is stored in SAM key entry number 9. Key type is AES-128 and PICC key.

SET = 2000; AES 128 key type.

ExtSET = 11; PICC key and use of diversification must (if this bit is not set then use of key diversification is optional with that key entry).

Table 4. Example - MIFARE Plus SL3 First Authentication

step	Indication		Data / Message	Comment
1	Send first authentication command to MIFARE Plus	>	70044000	Cmd = 0x70, in this example block number 11, (means Key A sector 2 is block nr. 0x4004)
2	Response of MIFARE Plus	<	909F3087182F94778DEB437FBF8D8AE8DC	The status byte 0x90 and 16-byte En (RndB).

step	Indication		Data / Message	Comment
3	C-APDU to SAM, 1st part of SAM_AuthenticateMFP command	>	80A30D001909019F3087182F94778DEB437FBF8D8AE8DC044555A961288000	Data = SAM key entry nr, version and 16-byte En (RndB). Here 7-byte UID (044555A9612880) is used as diversification input. Please note, the diversified key has to be stored in the MIFARE Plus. In this example in block 0x4004.
4	R-APDU from SAM	<	E867F59E464796779760B9084D616C826B028E99DD7A4A37C042C56413962BDE90AF	32-byte En(RndA+RndB´)+SW1SW2 (90AF)
5	Send 2nd part of authentication command to MIFARE Plus	>	72E867F59E464796779760B9084D616C826B028E99DD7A4A37C042C56413962BDE	Cmd = 0x72 and 32-byte En(RndA+RndB´); Use ISO/IEC 14443-4 (T=CL) frame.
6	Response of MIFARE Plus	<	90377272162B849E9734781E6E8C5B66A517D8F660D6F0CD66D91ED5F9490F7131	Status byte 0x90(success) and Ek(RndA´).
7	C-APDU to SAM, 2nd part of SAM_AuthenticateMFP command	>	80A3000020377272162B849E9734781E6E8C5B66A517D8F660D6F0CD66D91ED5F9490F713100	Data = Ek(RndA´). Put here Le = 0x00.
8	R-APDU from SAM	<	0000000000000000000000009000	PDCap + PCDCap + SW1SW2 = 9000, authentication is successful.

2.4.2 Example – MIFARE Plus SL3 Following Authentication

Similar as shown is section 2.3.2 or 2.5.1. In step 3, use the right block number.

2.4.3 Example – MIFARE Plus Read

The MIFARE Plus SL3 data/value access commands and responses require cryptogram calculation using SAM. Then these cryptograms are exchanged between MIFARE Plus and reader.

Table 5. Example - MIFARE Plus SL3 Read

step	Indication		Data / Message	Comment
1	SAM_ CombinedReadMFP C-APDU	>	8033000004**31080003**00	The MIFARE Plus read (encrypted, CMAC on command, CMAC on response). Cmd = 31, staring block number 08 (0800) and to read 3 blocks. Here used for command so bit number 0 of P1 has to be set to 0.
2	R-APDU of SAM	<	3D23D7C1D54980CF9000	The command cryptogram and status.
3	Read command to MIFARE Plus	>	310800033D23D7C1D54980CF	MIFARE Plus read command and calculated cryptogram from SAM.

step	Indication		Data / Message	Comment
4	Response of MIFARE Plus	<	9001B4C5DFF1EF0EFD845AB40DC28FF77E30327D1492712D7DB37AAC666EDB30E00637DAA81A051D4E843DAA4CB18B5FE668D31A68AA3D8361	Status 90 + 48 bytes encrypted data (as to read 3 blocks) + 8 byte CMAC.
5	SAM_ CombinedReadMFP C-APDU.	>	80330100399001B4C5DFF1EF0EFD845AB40DC28FF77E30327D1492712D7DB37AAC666EDB30E00637DAA81A051D4E843DAA4CB18B5FE668D31A68AA3D836100	To decrypt the data received from MIFARE Plus. Used for response, bit number 0 of P1 has to be set to 1.
6	R-APDU of the SAM	<	0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000009000	Plain 48 bytes data and status (successful). This data transfer can be made encrypted by using the secure messaging.

2.4.4 Example – MIFARE Plus Write

The MIFARE Plus SL3 data/value access commands and responses require cryptogram calculation using SAM. Then these cryptograms are exchanged between MIFARE Plus and reader.

Table 6. Example - MIFARE Plus SL3 Write

step	Indication		Data / Message	Comment
1	SAM_ CombinedWriteMFP C-APDU	>	8034000023**A1080000010203040506070809 0A0B0C0D0E0F101112131415161718191A1B1C1D1E1F**00	The MIFARE Plus write (encrypted, CMAC on command, CMAC on response). Cmd = A1, staring block number 08 (0800) and data to write =000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F. Here used for command so bit number 0 of P1 has to be set to 0.
2	R-APDU of SAM	<	9DFC4D442D3DC57E71DABC211337C8CC768CB8CFE37E0A8F47641C3F8D7E4DB3B2DB04AD9D3B3BD09000	Encrypted data and CMAC + status (9000)
3	Write command to MIFARE Plus	>	A108009DFC4D442D3DC57E71DABC211337C8CC768CB8CFE37E0A8F47641C3F8D7E4DB3B2DB04AD9D3B3BD0	MIFARE Plus write command and calculated cryptogram from SAM.
4	Response of MIFARE Plus	<	907C32C3FD70E45B2E	Status 90 + 8 byte CMAC.
5	SAM_ CombinedWriteMFP C-APDU.	>	8034010009907C32C3FD70E45B2E00	To verify the CMAC received from MIFARE Plus. Here used for response so bit number 0 of P1 has to be set to 1.

step	Indication		Data / Message	Comment
6	R-APDU of the SAM	<	9000	Status success. Although no response data, in the C-APDU Le has to be set 00.

2.4.5 Example – MIFARE Plus EV1 Virtual Card Selection

This example is only relevant for MIFARE Plus EV1 and MIFARE Plus EV2.

For each Virtual Card Selection Last (VCSL), two AES keys are required. One is the encryption key and other one is the CMAC key. In this example, key entry 1 and key entry 2 have been used. The keys are AES-128 and of PICC key class.

Table 7. Example - MIFARE Plus Virtual Card Selection

step	Indication		Data / Message	Comment
1	Virtual card select (VCS) command to MIFARE Plus	>	42A000000396564341FFFFFFFFFFFFFFFF	Cmd and 16-byte IID.
2	Response of the MIFARE Plus card	<	90	The response will be always 90 (OK), if the IID exists or not.
3	Virtual card select last (VCSL) command to MIFARE Plus	>	4BA000000396564341FFFFFFFFFFFFFFFF000102030405060708090A0B03010203	Cmd = 4B; 16-byte IID, 12-byte Rndq, 1 byte LenCap + 3-byte PCDCap. LenCap can be 00 to 03.
4	Response of MIFARE Plus	<	908EAEADAD2DACDEF06AA5B041B5F458A00D22EF0A204C2F2C	Status 90 + 16-byte encrypted info + 8-byte CMAC.
5	SAM_ VirtualCardSupportMFP C-APDU.	>	804100002D0101FF02FF000102030405060708090A0B8EAEADAD2DACDEF06AA5B041B5F458A00D22EF0A204C2F2C0301020300	Data field = 1 byte Duos (no of VCSL commands) in this example 01 + KeyNrEnc + KeyVEnc + KeyNrCMAC + KeyVCMAC + Rndq + response of MIFARE Plus (from step 4 except status) + LenCap + PCDCap (as used in step 3)
6	R-APDU of the SAM	<	0003000B046055A96128809000	SW1SW2 (9000) means successful. The data field = Status byte + Info byte + 2-byte PD Cap + UID of the VC.

2.5 SAM AV3 with MIFARE Plus EV1 and EV2 in SL3 - EV1 secure messaging

MIFARE Plus EV1 and MIFARE Plus EV2 incorporates support for two different Secure Messaging systems, known as EV0 and EV1. Secure Messaging EV0 is the legacy secure messaging from MIFARE Plus EV0 (X, S, SE) and therefore directly supported by SAM AV3.

If operating on an environment that includes both MIFARE Plus EV0 (X, S, SE), MIFARE Plus EV1 or and MIFARE Plus EV2 and SAM AV3 support is requested, usage of Secure Messaging EV0 is recommended.

For this scenario, no changes are needed for supporting MIFARE Plus EV0 cards, but MIFARE Plus EV1 and EV2 require that at the beginning of an authentication transaction (when the AuthenticateFirst command is sent) the requested secure messaging to be selected.

This is done by setting byte PCDCap2.1 to 0 (Secure Messaging EV0 selected) or 1 (Secure Messaging EV1 selected). For this reason, the AuthenticateFirst always requires the PCDCap2.1 byte to be transmitted.

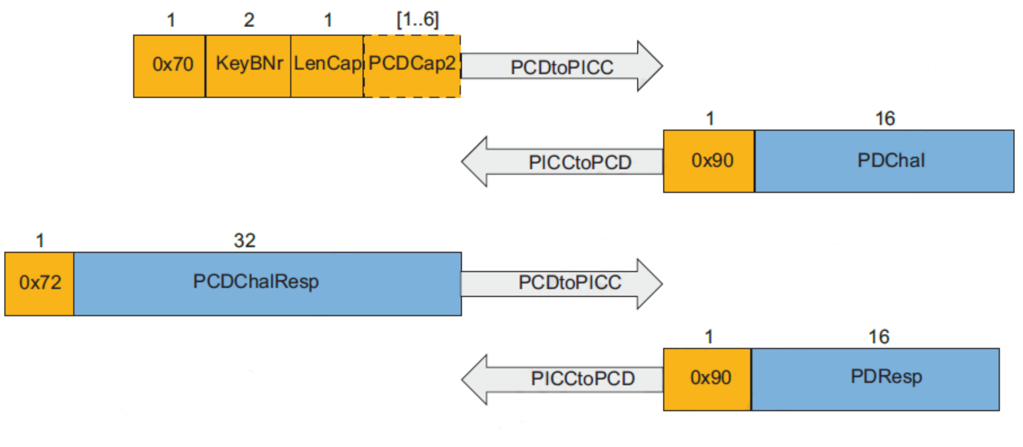

Figure 2. MIFARE Plus EV1: AuthenticateFirst

For Systems only using MIFARE Plus EV1 or MIFARE Plus EV2, EV1 secure messaging will be applied per default.

2.5.1 Authentication using MIFARE Plus EV1 Secure Messaging

This example is only relevant for MIFARE Plus EV1 and MIFARE Plus EV2

The following example does the same as the example in section Table 4, but using the EV1 secure messaging. Therefore, the PCDCaps need to be transmitted at the AuthenticateFirst command.

Table 8. Example - MIFARE Plus SL3 First Authentication using EV1 secure messaging

step	Indication		Data / Message	Comment
1	Send first authentication command to MIFARE Plus EV1, including 6 Bytes of PCDCap	>	700440060**10000000000**	Cmd = 0x70, in this example block number 11, (means Key A sector 2 is block nr. 0x4004), PCDCaps2.1 =0x01, means, EV1 secure messaging is used
2	Response of MIFARE Plus	<	90B236D3943BAED26D1C5FB38FCE07E116	The status byte 0x90 and 16-byte En (RndB).
3	C-APDU to SAM, 1st part of SAM_AuthenticateMFP command	>	80A30D00160901B236D3943BAED26D1C5FB38FCE07E116B3E16A6000	Data = SAM key entry nr, version and 16-byte En (RndB). Here 4-byte UID (B3E16A60) is used as diversification input. Please note, the diversified key has to be stored in the MIFARE Plus EV1. In this example in block 0x4004.

step	Indication		Data / Message	Comment
4	R-APDU from SAM	<	7030A6384A10B80AC63E0C9D9BE983687DA7CCD00C8565617DE5BDB542AC350590AF	32-byte En(RndA+RndB´)+SW1SW2 (90AF)
5	Send 2nd part of authentication command to MIFARE Plus	>	727030A6384A10B80AC63E0C9D9BE983687DA7CCD00C8565617DE5BDB542AC3505	Cmd = 0x72 and 32-byte En(RndA+RndB´); Use ISO/IEC 14443-4 (T=CL) frame.
6	Response of MIFARE Plus	<	90F330A14D33DC20BCC7B26DD4326659B3FE8754395698099074DAAB4CBBD4D422	Status byte 0x90(success) and Ek(RndA´).
7	C-APDU to SAM, 2nd part of SAM_AuthenticateMFP command	>	80A3000020F330A14D33DC20BCC7B26DD4326659B3FE8754395698099074DAAB4CBBD4D42200	Data = Ek(RndA´). Put here Le = 0x00.
8	R-APDU from SAM	<	0100000000000100000000009000	PDCap + PCDCap + SW1SW2 = 9000, authentication is successful.

As one can clearly see, the secure messaging Type does not make any difference to the command flow, except for the added PCDCap Bytes in the initial command. Therefore, all other examples for EV1 secure messaging are skipped.

3 References

1. **Data sheet –** Data sheet of MIFARE SAM AV3, doc nr. 3235xx.
2. **System guidance manual – MF4SAM3 (MIFARE SAM AV3)**, document number 5385xx.
3. **Data sheet –** MIFARE Plus EV1, document number 3226xx.
4. **Data sheet –** MIFARE Plus EV2, document number 5223xx
5. **Application note** – **AN12695 – MIFARE SAM AV3 – Quick Start up Guide**, document number 5210xx, https://www.nxp.com/docs/en/application-note/AN12695.pdf.
6. **Application note** – **AN5212 – MIFARE SAM AV3 – Key Management and Personalization**, document nr. 5212xx.
7. **Application note – Symmetric Key Diversifications**, document number 1653xx.
8. **Application note – AN5217 – MIFARE SAM AV3 for MIFARE Classic,** document number 5217xx
9. **Application note – AN12704 – MIFARE SAM AV3 Host communication,** document number 5213xx, https://www.nxp.com/docs/en/application-note/AN12704.pdf.

4 Legal information

4.1 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.

4.2 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.

Security — While NXP Semiconductors has implemented advanced security features, all products may be subject to unidentified vulnerabilities. Customers are responsible for the design and operation of their applications and products to reduce the effect of these vulnerabilities on customer's applications and products, and NXP Semiconductors accepts no liability for any vulnerability that is discovered. Customers should implement appropriate design and operating safeguards to minimize the risks associated with their applications and products.

4.3 Licenses

ICs with DPA Countermeasures functionality

LICENSED DPA COUNTERMEASURES™

NXP ICs containing functionality implementing countermeasures to Differential Power Analysis and Simple Power Analysis are produced and sold under applicable license from Cryptography Research, Inc.

4.4 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.

NXP — wordmark and logo are trademarks 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: 12 May 2020
Document identifier: AN12706
Document number: 521412