AN12697

MIFARE SAM AV3 for NTAG 424 DNA

Rev. 1.1 — 8 January 2020 Application note
521811 COMPANY PUBLIC

Document information

Information	Content
Keywords	MIFARE SAM AV3, NTAG 424 DNA, NTAG, DNA, SUN
Abstract	This application note shows the usage of NTAG 424 DNA features in combination with a MIFARE SAM AV3

Revision history

Rev	Date	Description
1.1	20200108	AN number changed, security status changed into “Company Public”
1.0	20190702	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 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 NTAG 424 DNA products. 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.

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

1.2 Abbreviation

Refer to application note “MIFARE SAM AV3 – Quick Start up Guide” [3].

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).

Gray rows contain communication between the host and the PICC, which is out of scope for this document

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.

1.4 S interface

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

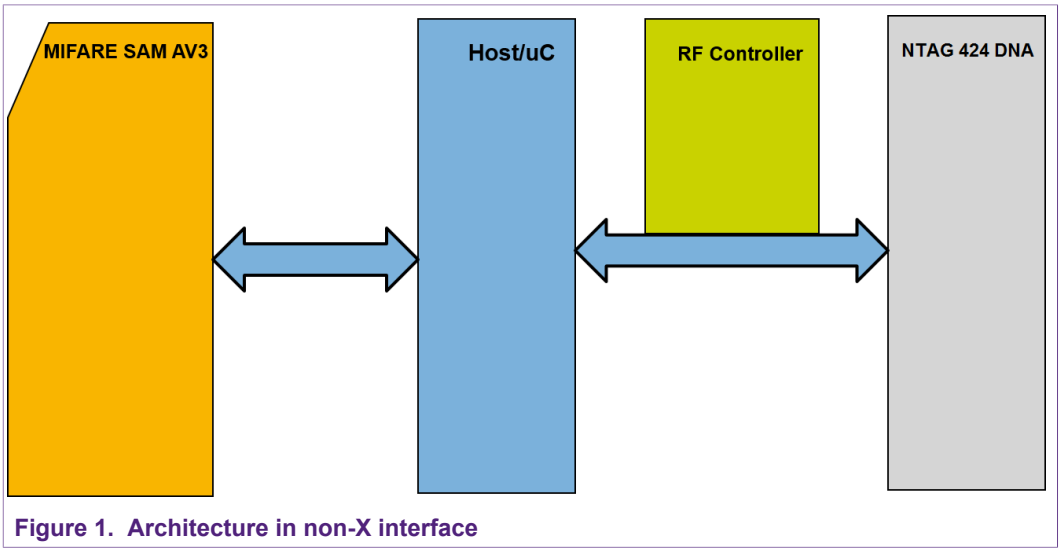

Figure 1. Architecture in non-X interface

2 NTAG 424 DNA Authentication

MIFARE SAM AV3 can be used in combination with NTAG 424 DNA to perform, e.g., mutual authentication.

The following example shows the authentication using the SAM_AuthenticatePICC command.

The NTAG 424 DNA accepts AES-128 keys. The authentication mode cn be chosen to be AES or LRP (using AES Keys). For details information about LRP, please see [LRP specification],[NTAG 424 DNA - LRP mode]

2.1 Authentication example

This example authenticates an NTAG 424 DNA using SAM AV3. The example uses as plain sample, with all 5 keys written as all 0x00, AES128 keys. The authentication is performed with the Master Key number 0x00.

The Key in the SAM shall have the following configuration:

- Key Class = PICC
- Key Type = AES128
- Key Value = 0x00000000000000000000000000000000
- Key Version = 0x00
- KeyNoCEK and KeyNoAEK does not matter, but of course, the Key should be accessible.
- In this example, the Key is stored on Key No. 0x05[1]

Table 1. Example - Authentication of NTAG 424 DNA

step	Indication		Data / Message	Comment
1	Activate the NTAG 424 DNA up to ISO/IEC 14443-4.			
2	Perform ISO_Select with DF name D2760000850101 to select the application			
3	Send to NTAG 424 DNA	>	9071000002000000	Authenticate Command: The command needs to be sent in ISO7816 APDU format. CLA = 90, INS = 71, P1 and P2 = 00, Lc = 02. The data passed is 0000, which is Key number of the NTAG 424 DNA Key to authenticate with, and the Capability length, which is 00 in this example.
4	Receive E(Kx, RndB)	<	09259A581AA31F76A1C7 C3D88F06457C91AF	RndB + SW1SW2

1 The command for creating this key can be found in the Section 5

step	Indication		Data / Message	Comment
5	Send authenticate command to SAM AV3	>	800A80001305000009259A581AA31F76A1C7C3D88F06457C00	Command instruction 0A. P1 = 80, which means EVx authentication mode with AuthenticateFirst command. P2=00. The data field contains the SAM Key number (05), SAM Key Version (00), the AuthMode (00), which decides if AES or LRP is used, and the encrypted RndB. Le = 00
6	SAM AV3 answers with E(Kx, RndA || RndB')	<	260EEBF10FF7E47885E50F98ED265E8209686357304590DAF264755EFC96396990AF	The finished cryptogram of E(Kx, RndA || RndB') with SW1Sw2. This needs to be passed to the NTAG 424 DNA.
7	Send E(Kx, RndA || RndB') to NTAG 424 DNA	>	90AF000020260EEBF10FF7E47885E50F98ED265E8209686357304590DAF264755EFC96396900	The E(Kx, RndA || RndB') is sent to the NTAG 424 DNA, again with ISO7816 command format. CLA = 90, INS = AF, P1 and P2 = 00. The data field contains the cryptogram. Le = 00
8	NTAG 424 DNA answers with E(Kx, TI || RndA' || PDcap2 || PCDcap2)	<	8588E1E7C33CB3667C9BF811683ECFB17EA24FDD22D02064D06773986A5D835D9100	E(Kx, TI || RndA' || PDcap2 || PCDcap2) from NTAG 424 DNA. SW1SW2=9100, indicating success from NTAG 424 DNA side.
9	Send E(Kx, TI || RndA' || PDcap2 || PCDcap2) to SAM AV3	>	800A0000208588E1E7C33CB3667C9BF811683ECFB17EA24FDD22D02064D06773986A5D835D00	Provide the cryptogram to the SAM. The SAM will verify the RndA and provide back the Capability vector PDcap2||PCDcap2.
10	Receive PDcap2|| PCDcap2	<	00000000000000000000009000	PDcap2||PCDcap2 and SW1SW2 = 9000, indicating success of the mutual authentication.

The NTAG 424 DNA is now authenticated. The SAM AV3 has now every relevant parameter to apply EV2 secure messaging, until the next kill authentication command is performed.

3 NTAG 424 DNA with MIFARE SAM AV3 light

3.1 Authentication example using SAM AV3 Light

This example authenticates an NTAG 424 DNA using SAM AV3 **Light**. Compared to the full version, the SAM AV3 Light does not support MIFARE DESFire and MIFARE Plus cryptography and secure messaging. Therefore the authentication sequence and following secure messaging steps need to be performed using the Offline Crypto features of SAM AV3

The example uses a fresh NTAG 424 DNA sample, all PICC keys still have the default values of all 0x00, the authentication is performed with the Master Key number 0x00.

The Key in the SAM shall have the following configuration:

- Key Class = **OfflineCrypto**
- Key Type = AES128
- Key Value = 0x00000000000000000000000000000000
- Key Version = 0x00
- KeyNoCEK and KeyNoAEK does not matter, but of course, the Key should be accessible.
- In this example, the Key is stored on Key No. 0x05[2]

Table 2. Example - Authentication of NTAG 424 DNA

step	Indication		Data / Message	Comment
1	Activate the NTAG 424 DNA up to ISO/IEC 14443-4.			
2	Perform ISO_Select with DF name D2760000850101 to select the application			
3	Send to NTAG 424 DNA	>	9071000002000000	Authenticate Command: The command needs to be sent in ISO7816 APDU format. CLA = 90, INS = 71, P1 and P2 = 00, Lc = 08. The data passed is 0000, which is Key number of the NTAG 424 DNA Key to authenticate with, and the Capability length, which is 06, followed by 6 Bytes of zeroes.
4	Receive E(Kx, RndB) from NTAG 424 DNA	<	26CF42B32A3A4DDF771 96313BC32A6FF91AF	RndB + SW1SW2
5	Send ActivateOfflineKey to SAM AV3	>	80010000020500	Activate the Key for offline use, KeyNo 05, KeyVersion 00
6	R-APDU from SAM AV3	<	9000	success
7	SAM_DecipherOffline	>	800D00001026CF42B32A 3A4DDF77196313BC32A 6FF00	Decipher offline command to get RndB using the currently activated OfflineKey
8	Receive RndB	<	9C24DF43F7C30F6E789 ADCAF786982E89000	Receive RndB + SW1SW2

2 The command for creating this key can be found in the Section 5

step	Indication		Data / Message	Comment
9	GetRandom from SAM AV3	>	8084000010	Create 16 Byte RndA using the SAM_GetRandom command
10	Receive RndA from SAM AV3	<	F375D897E5971E24AC6 6134980BCF19B9000	RndA + SW1SW2
11	Generate RndB'	=	24DF43F7C30F6E789AD CAF786982E89C	RndB' is a left rotation of RndB. In other words, the first Byte of RndB is moved to the end.
12	SAM_EncipherOffline of RndA||RndB'	>	800E000020F375D897E5 971E24AC66134980BCF 19B24DF43F7C30F6E78 9ADCAF786982E89C00	SAM_EncipherOffline command used to encrypt RndA||RndB' using the currently activated OfflineKey.
13	Receive the Cryptogram from SAM	<	DF40814785B249C83C0 03B9275F18600F90B9DC F3DD963E09DF08F3CE7 9B62E89000	E(Kx, RndA||RndB') + SW1SW2
14	Send Cryptogram to NTAG 424 DNA	>	90AF000020DF40814785 B249C83C003B9275F186 00F90B9DCF3DD963E09 DF08F3CE79B62E800	The E(Kx, RndA || RndB') is sent to the NTAG 424 DNA, again with ISO7816 command format. CLA = 90, INS = AF, P1 and P2 = 00. The data field contains the cryptogram. Le = 00
15	NTAG 424 DNA answers with E(Kx, TI || RndA' || PDcap2 || PCDcap2)	<	17FF1A89931D545B3A77 4E3297ACE0142DE0946 F16CD0F29CD9BDA1F01 3A151C9100	E(Kx, TI || RndA' || PDcap2 || PCDcap2) from NTAG 424 DNA. SW1SW2=9100, indicating success from NTAG 424 DNA side.
16	SAM_DecipherOffline	>	800D00002017FF1A8993 1D545B3A774E3297ACE 0142DE0946F16CD0F29 CD9BDA1F013A151C00	SAM_DecipherOffline command to decrypt E(Kx, TI || RndA' || PDcap2 || PCDcap2)
17	Receive TI || RndA' || PDcap2 || PCDcap2 from SAM AV3	<	4D5F8B4E75D897E5971 E24AC66134980BCF19B F3000000000000000000 000009000	Receive TI = 4D5F8B4E, RndA', PDcap2 || PCDcap2 all zeroes and SW1SW2 indicating success(9000)
18	Verify RndA	=	F375D897E5971E24AC6 6134980BCF19B	Right rotate RndA' to obtain RndA. **The authentication was successful.**
19	Prepare RAM Key entry E0 in SAM AV3	>	80C1E08F40000000000 00000000000000000000 00000000000000000000 00000000000000000000 00000000000000000000 0000000000000FF20000 001020400FEFE	This command will preparate the RAM Key entry E0 for the Session ENC Key. The key class needs to be OfflineCrypto, and KeyType AES128. Also, KeyNoCEK, KeyVSEK, KeyNoAEK and KeyVAEK need to be exact the same as the source Key.
20	R-APDU from SAM AV3	<	9000	success

step	Indication		Data / Message	Comment
21	Prepare RAM Key entry E1 in SAM AV3	>	80C1E18F400000000000 00000000000000000000 00000000000000000000 00000000000000000000 00000000000000000000 00000000000000FF20000 001020400FEFE	
22	R-APDU from SAM AV3	<	9000	success
23	Build input for session key generation K_{ENC}	=	A55A00010080F3750F6E 789ADCAF786982E8AC6 6134980BCF19B	See Section 5.1 for detailed Information
24	Build input for session key generation K_{MAC}	=	5AA500010080F3750F6E 789ADCAF786982E8AC6 6134980BCF19B	See Section 5.1 for detailed Information
25	SAM_DeriveKey	>	80D700001D0500E0A55A 00010080F3750F6E789A DCAF786982E8AC66134 980BCF19B	SAM_DeriveKey command to store K_{ENC} in Key E0 (first RAM Key). CLA = 80, INS = D7, P1 and P2 = 00. The data field contains the source key and version (05, 00) and the destination Key (E0). The key settings for the destination Key need to be exactly the same as for the source Key.
26	R-APDU from SAM AV3	<	9000	success
27	SAM_DeriveKey	>	80D700001D0500E15AA5 00010080F3750F6E789A DCAF786982E8AC66134 980BCF19B	SAM_DeriveKey command to store K_{MAC}in Key E1 (second RAM Key). CLA = 80, INS = D7, P1 and P2 = 00. The data field contains the source key and version (05, 00) and the destination Key (E0). The key settings for the destination Key need to be exactly the same as for the source Key.
28	R-APDU from SAM AV3	<	9000	success

The NTAG 424 DNA is now authenticated. Both session keys are stored in the RAM Key entries E0 and E1 for further use. Please note: The RAM Key values are not persistent! After a SAM reset, the procedure needs to be repeated.

4 SAM AV3 and Secure Unique NDEF (SUN) Messaging

The NTAG 424 DNA offers a feature which allows confidential and integrity protected data exchange, without a preceding authentication. This feature is called "Secure unique NDEF" (SUN), or "Secure Dynamic Messaging" (SDM).

A secure dynamic message can be of many different kinds, an example is a URL.

https://ntag.nxp.com/424?
e=EF963FF7828658A599F3041510671E88&c=94EED9EE65337086

For more detailed information, have a look at [Application note - NTAG 424 DNA Features and Hints]

4.1 Verify cryptogram

The above given example is a URL[3] containing the Host, some encrypted data(e=...) and a CMAC(c=...). This data needs to be decrypted, and the CMAC needs to be verified. SAM AV3 Offline Crypto can be used for both of this in one go.

The Key in the SAM shall have the following configuration:

- Key Class = **OfflineCrypto**
- Key Type = AES128
- Key Value = 0x00000000000000000000000000000000
- Key Version = 0x00
- KeyNoCEK and KeyNoAEK does not matter, but of course, the Key should be accessible.
- In this example, the Key is stored on Key No. 0x05[4]

Table 3. Example - decrypting SUN message

step	Indication		Data / Message	Comment
1	encrypted message	=	EF963FF7828658A599F3041510671E88	encrypted message out of the NDEF
2	SAM_ActivateOffline	>	80010000020500	Activate the key for offline use
3	R-APDU	<	9000	success
4	SAM_DecipherOffline	>	800D000010EF963FF7828658A599F3041510671E8800	Decipher the encrypted message
5	Cleartext message	<	C704DE5F1EACC0403D0000DA5CF609419000	Deciphered message from NTAG 424 DNA and SW1SW2 = 9000
6	PICCDataTag	=	C7	1100 0111, UID mirrored (bit7), SDMReadCtr mirrored (bit6), UIDLength 7 byte (bit3-0)
7	UID	=	04DE5F1EACC040	
8	SDMReadCtr	=	3D0000	
9	Random Padding	=	DA5CF60941	
Session Key Generation				

3 The SUN message does not necessarily need to be a URL, this is just here chosen as an example
4 The command for creating this Key can be found in the Section 5. It is the same Key as for example No. 2.

step	Indication		Data / Message	Comment
10	SV2 = 3CC3 0001 0080 [UID] [SDMReadCtr] [ZeroPadding]	=	3CC30001008004DE5F1 EACC0403D0000	Input vector for session key generation, $K_{SesSDMFileReadMAC}$ = MAC($K_{SDMFileRead}$; SV2)
11	Prepare RAM Key	>	80C1E08F400000000000 0000000000000000000000 0000000000000000000000 0000000000000000000000 0000000000000000000000 00000000000000FF20000 0000004000000	Prepared the RAM Key E0 to hold the session key to be generated. The key settings have to be the same as the source key.
12	R-APDU	<	9000	success
13	SAM_DeriveKey	>	80D70000130500E03CC3 0001008004DE5F1EACC 0403D0000	Derive the $K_{SesSDMFileReadMAC}$from the source key 0x05, and stores it into RAM key entry 0xE0.
14	R-APDU	<	9000	success
15	$K_{SesSDMFileReadMAC}$	=	3FB5F6E3A807A03D5E3 570ACE393776F	NOTE: This key is written here just for the example, in real application, this key will only stay in the SAM AV3
16	SAM_ActivateOffline	>	8001000002E000	Activate the generated RAM-key for offline use.
17	R-APDU	<	9000	success
18	GenerateMAC	>	807C008000	MACt($K_{SesSDMFileReadMAC}$; DynamicFileData[SDMMACInputOffset :: SDMMACOffset - 1]) (detailed information in [6]. In this example: **CMACInputOffset == CMACOffset, therefore, a MAC over zero length input is created**. P1=0x08 indicates that "MFP trucation" is selected. This is the NXP standard for CMAC trucation.
19	SDMMAC	<	94EED9EE653370869000	returns the SDMMAC and SW1SW2 = 9000 indicating success.
20	compare	=	Generated SDMMAC and provided MAC are identical	The transaction is valid.

5 Appendix

5.1 Apendix A: Session Key Generation

The input data used to calculate both the encryption and the MAC session key use the following fields, as defined in the NIST SP 800-108.

- a 2-byte label, distinguishing the purpose of the key: 5AA5h for MACing and A55Ah for encryption
- a 2-byte counter, fixed to 0001h as only 128-bit keys are generated.
- a 2-byte length, fixed to 0080h as only 128-bit keys are generated.
- a 26-byte context, constructed using the two random numbers exchanged, RndA and RndB

Following steps are performed to generate the encryption session key for confidentiality protection

1. Retrieve the bit streams:
2. A = RndA[15_d ... 14_d]
3. B = RndA[13_d ... 8_d]
4. C = RndB[15_d ... 10_d]
5. E = RndB[9_d ... 0_d]
6. F = RndA[7_d ... 0_d]
7. Perform an XOR-operation on value B and C to retrieve D.
   D = B XOR C = RndA[13_d ... 8_d] XOR RndB[15_d ... 10_d]
8. Concatenate the items to obtain the session key base:

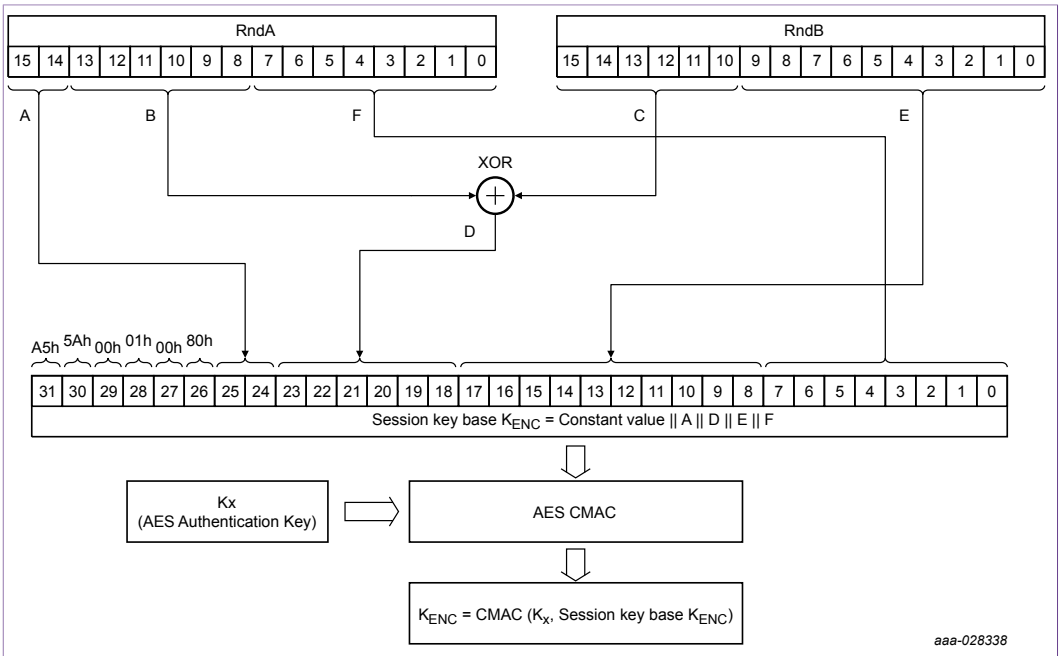

Figure 2. K_{ENC} creation

Session key base for K_{ENC} = A5h || 5Ah || 00h || 01h || 00h || 80h || A || D || E || F

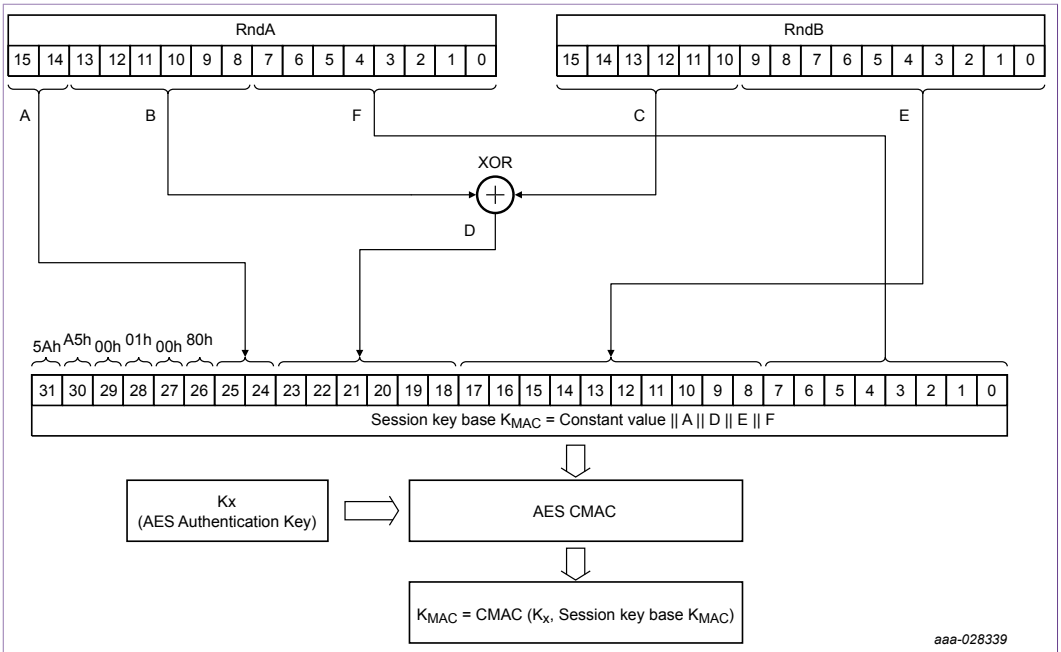

Figure 3. K_{MAC} creation

Session key base for K_{MAC} = 5Ah || A5h || 00h || 01h || 00h || 80h || A || D || E || F

The session key base is then used as an input for the SAM_DeriveKey command.

5.2 Appendix B: Change Key commands

Create the key for example in Section 2.1

Table 4. ChangeKey Command for Example 1

Data	Comment
80C108FF40	Command Header
00000000000000000000000000000000	KeyA
11111111111111111111111111111111	KeyB
22222222222222222222222222222222	KeyC
000000000000FF20000001020100FEFE	Settings (Important: PICC Key Class)

Create the key for example in Section 3.1

Table 5. ChangeKey Command for Example 2

Data	Comment
80C108FF40	Command Header
00000000000000000000000000000000	KeyA
11111111111111111111111111111111	KeyB
22222222222222222222222222222222	KeyC
000000000000FF20000001020400FEFE	Settings (Important: OfflineCrypto Key Class)

Both above commands will insert a key in the key entry 0x05 on the SAM. These keys can be used for the examples above.

NOTE: When preparing the RAM Keys in Step 19, make sure that the settings are the same as for the source Key entry.

6 References

1. **Data sheet –** Data sheet of MIFARE SAM AV3, document number 3235xx.
2. **System guidance manual – MF4SAM3 (MIFARE SAM AV3)**, document number 5385xx.
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. **Leakage Resilient Primitive (LRP) Specification (1.1)**, document number 4660xx.
5. **Data sheet –** Data sheet of NTAG 424 DNA, doc nr. 4654xx.
6. **Application note** – **NTAG 424 DNA features and hints**, document number 5072xx.
7. **Application note** – **NTAG 424 DNA - LRP mode**, document number 5244xx.

7 Legal information

7.1 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.

7.2 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.

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 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.

7.3 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.

7.4 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.

ICODE and I-CODE — are trademarks of NXP B.V.

UCODE — 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.

NTAG — is a trademark of NXP B.V.

Tables

Figures

Contents

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

Date of release: 8 January 2020
Document identifier: AN12697
Document number: 521811