AN12702

MIFARE SAM AV3 – For general purpose cryptography

Rev. 1.1 — 7 July 2020 Application note

522111 COMPANY PUBLIC

Document information

Information	Content
Keywords	MIFARE SAM AV3, TDEA, AES, general purpose cryptography
Abstract	This application note presents some examples of using MIFARE SAM AV3 for general purpose cryptography.

Revision history

Rev	Date	Description
1.1	20200707	• AN number changed, security status changed into "COMPANY PUBLIC" • Typo correction in ECC example
1.0	20190116	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 general purpose cryptography. 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).

Table 1. C-APDU:

CLA	INS	P1	P2	Lc	Data (nc)	Le

Table 2. 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 SAM is the General purpose crypto unit

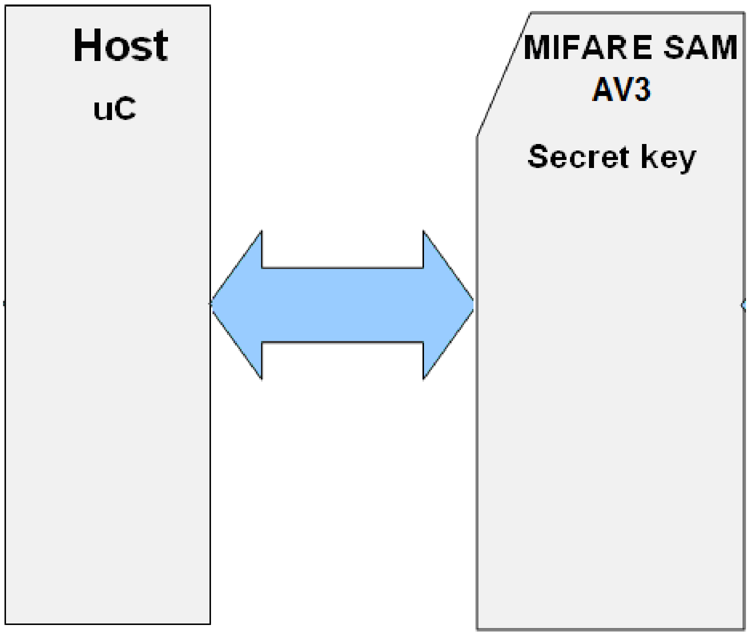

Figure 1. SAM for general purpose cryptography

2 Using MIFARE SAM AV3 for General Purpose Cryptography

MIFARE SAM AV3 can be used as a general purpose crypto machine to calculate different standard cryptography. The SAM can be considered a black-box containing the secret key securely can be used for the cryptogram (encryption, decryption, generate/ verify CMAC) calculation.

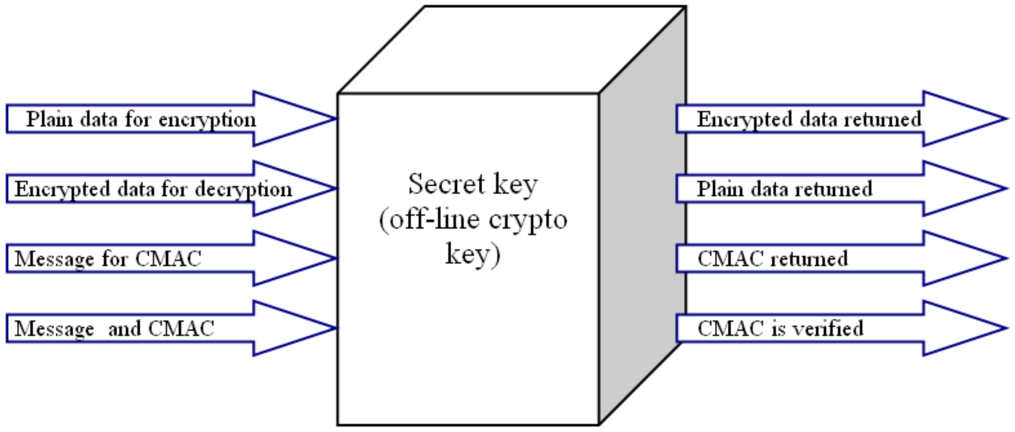

Figure 2. SAM is black-box for cryptography

The communication between the host and the SAM can be made secure as well. Please refer to [8] for detail.

2.1 Downloading the Offline Crypto Keys to SAM from Host

Downloading of different keys is explained in [5]. The SAM key entry settings are different for different types of crypto calculations. In the following table different options are shown:

Table 3. SAM Key Entry setting for different offline crypto keys

SAM Key entry setting	Bit value for “Offline Crypto Key”
SET bits	
b0: Allow dumping session key.	‘0’
b1: RFU must be set to 0.	‘0’
b2: Keep IV	‘0’ or ‘1’ (based on requirement)
b5b4b3: Key type	‘011’: 3TDEA ISO 10116 or ‘100’: AES 128 or ‘101’: AES 192 or ‘110’: TDEA ISO 10116 (32-bit CRC, 8-byte MAC) (based on requirement)
b7b6: RFU must be set to 0	‘00’
b8: Host Auth Key for unlocking the LC	‘0’
b9: Disable key entry	‘0’
b10: Lock Key	‘0’

SAM Key entry setting	Bit value for “Offline Crypto Key”
b11: Disable SAM_ ChangeKeyPICC	‘0’
b15b14b13b12	‘0000’ (or based on requirement)
ExtSET bits	
b2b1b0: Key class	‘100’
b3: Allow dumping secret key. Not recommended to set.	‘0’
b4: Restricted for diversification.	‘0’ or ‘1’ based on requirement.

2.2 Steps for using SAM as General purpose cryptography

The stored key needs to activate before using it for crypto calculation.

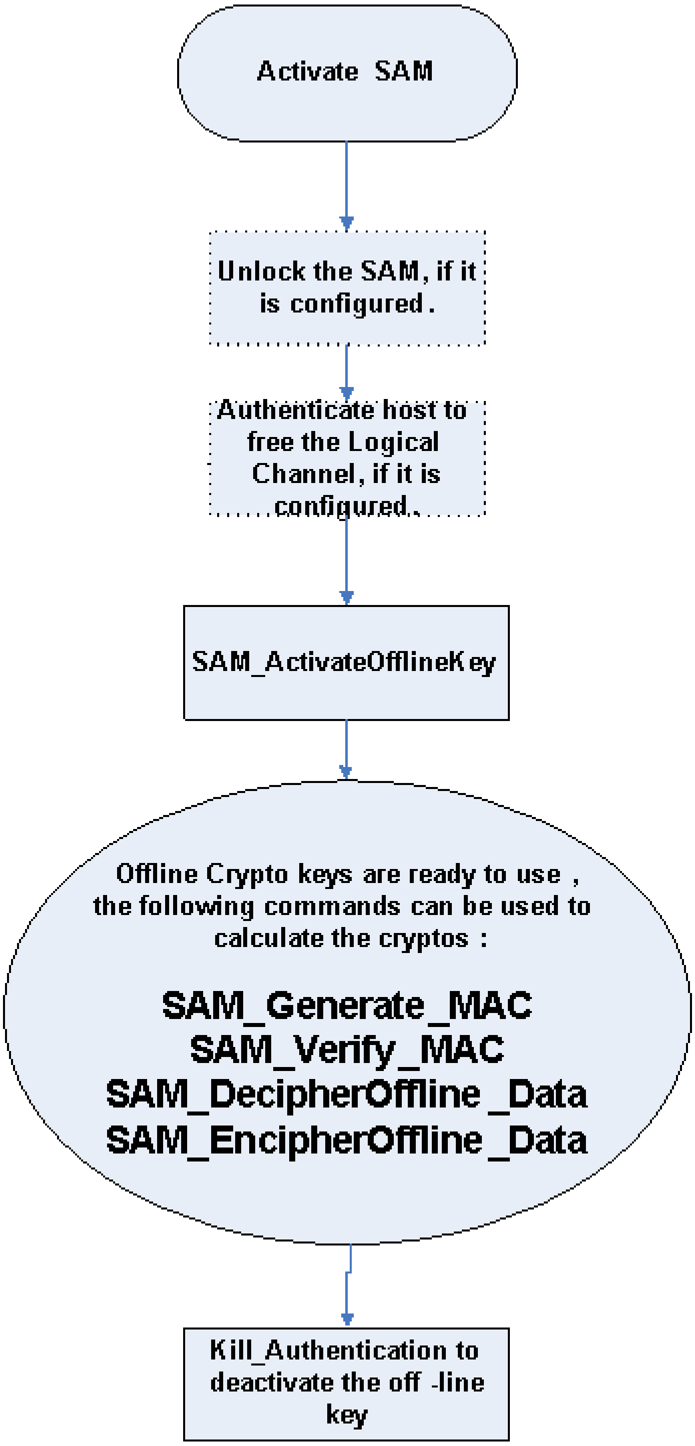
Activate SAM
Unlock the SAM, if it is configured.
Authenticate host to free the Logical Channel, if it is configured.
SAM_ActivateOfflineKey
Offline Crypto keys are ready to use , the following commands can be used to calculate the cryptos :
SAM_Generate_MAC
SAM_Verify_MAC
SAM_DecipherOffline_Data
SAM_EncipherOffline_Data
Kill_Authentication to deactivate the off -line key

Figure 3. Command flow for using SAM as a general purpose crypto

2.3 General purpose cryptography examples

Key entry number 6 which has the following setting, has been used in these examples.

Key Version A = 00
Key Version B = 01

Key Version C = 02
DF_AID = 000000
DF_KeyNo = 00
KeyNoCEK = 00
KeyVCEK = 00
RefNoKUC = FF

SET = 2000

DO NOT allow dump Session key
DO NOT allow crypto with secret key
DO NOT Keep IV
Key type: AES 128

ExtSET = 04

Off-line crypto key
Diversification is not mandatory

2.3.1 SAM_ActivateOfflineKey command example

Table 4. SAM_ActivateOfflineKey command Example

step	Indication		Data / Message	Comment
1	SAM_ ActivateOfflineKey C-APDU	>	80010000020601	P1 = 00; no key diversification. Data field is the SAM key entry number and version number.
2	SAM_ ActivateOfflineKey R-APDU	<	9000	The key entry number 6 with version 01 is ready for off-line crypto calculation.

2.3.2 SAM_EncipherOffline_Data command example

For reference the secret key of SAM key entry number 06, version 01 = “11111111111111111111111111111111”.

Table 5. SAM_EncipherOffline_Data command Example

step	Indication		Data / Message	Comment
1	Plain data to encrypt	=	0102030405060708090A0B0C0D0E0F10111213141516	22 bytes data for encryption
2	Padding has to be added by the user	=	0102030405060708090A0B0C0D0E0F1011121314151600000000000000000000	10 bytes padding is added to the plain data to make it multiple of block size. (AES block size = 16 and for TDES block size = 8, the key type defines the crypto mode). The padding according to ISO9797-1 method 1 or 2 can be given by the user.
3	SAM_ EncipherOffline_ Data C-APDU	>	800E0000200102030405060708090A0B0C0D0E0F10111213141516000000000000000000000000	Data field is the plain text (multiple block size).

step	Indication		Data / Message	Comment
4	SAM_ ActivateOfflineKey R-APDU	<	C82690652D9040F8A91FB65E634641D74280DED7E0589CA05CFE6293885184499000	Encrypted data and SW1SW2.
5	Encrypted data	=	C82690652D9040F8A91FB65E634641D74280DED7E0589CA05CFE629388518449	Encrypted data using the secret key stored in the SAM.

2.3.3 SAM_DecipherOffline_Data command example

For reference the secret key of SAM key entry number 06, version 01 = “11111111111111111111111111111111”.

Table 6. SAM_DecipherOffline_Data command Example

step	Indication		Data / Message	Comment
1	Encrypted data for decryption	=	C82690652D9040F8A91FB65E634641D74280DED7E0589CA05CFE629388518449	Encrypted using the secret key stored in SAM
2	SAM_ DecipherOffline_ Data C-APDU	>	800D000020C82690652D9040F8A91FB65E634641D74280DED7E0589CA05CFE62938851844900	Data field is the encrypted data, must be multiple of block size.
3	SAM_ ActivateOfflineKey R-APDU	<	0102030405060708090A0B0C0D0E0F10111213141516000000000000000000009000	Plain data with padding(if any)+SW1SW2
4	Plain data	=	0102030405060708090A0B0C0D0E0F10111213141516	22 bytes plain data

2.3.4 SAM_Generate_MAC command example

For reference the secret key of SAM key entry number 06, version 01 = “11111111111111111111111111111111”.

Table 7. SAM_Generate_MAC command Example

step	Indication		Data / Message	Comment
1	Message	=	0102030405060708090A0B0C0D0E0F10111213141516	22 byte message
2	SAM_Generate_ MAC C-APDU	>	807C0008160102030405060708090A0B0C0D0E0F1011121314151600	P2 = the CMAC length (here 08), Data field is the message.
3	SAM_Generate_ MAC R-APDU	<	994F7D6D100435C29000	8-byte CMAC + SW1SW2.
4	CMAC	=	994F7D6D100435C2	Standard (NIST 800-38B) CMAC calculated using the secret key stored in the SAM.

2.3.5 SAM_Verify_MAC command example

For reference the secret key of SAM key entry number 06, version 01 = “11111111111111111111111111111111”.

Table 8. SAM_Verify_MAC command Example

step	Indication		Data / Message	Comment
1	Message	=	0102030405060708090A0B 0C0D0E0F10111213141516	22 byte message
2	CMAC	=	994F7D6D100435C2	8-byte CMAC
3	SAM_Verify_ MAC C-APDU	>	805C00081E010203040506 0708090A0B0C0D0E0F101 11213141516994F7D6D100 435C2	P2 = 08 means 8-byte standard CMAC to be verified, data field is the message and CMAC.
4	SAM_Verify_ MAC R-APDU	<	9000	CMAC is verified successfully.

2.4 Using General Purpose Cryptography in applications

To increase the level of security for confidential data stored in cards (may be built-in security offered by the card is not very strong), the application may calculate seal (CMAC) and or encrypt data before storing it in the card.

Figure 4 shows a widely used way of seal (MAC) calculation for storage.

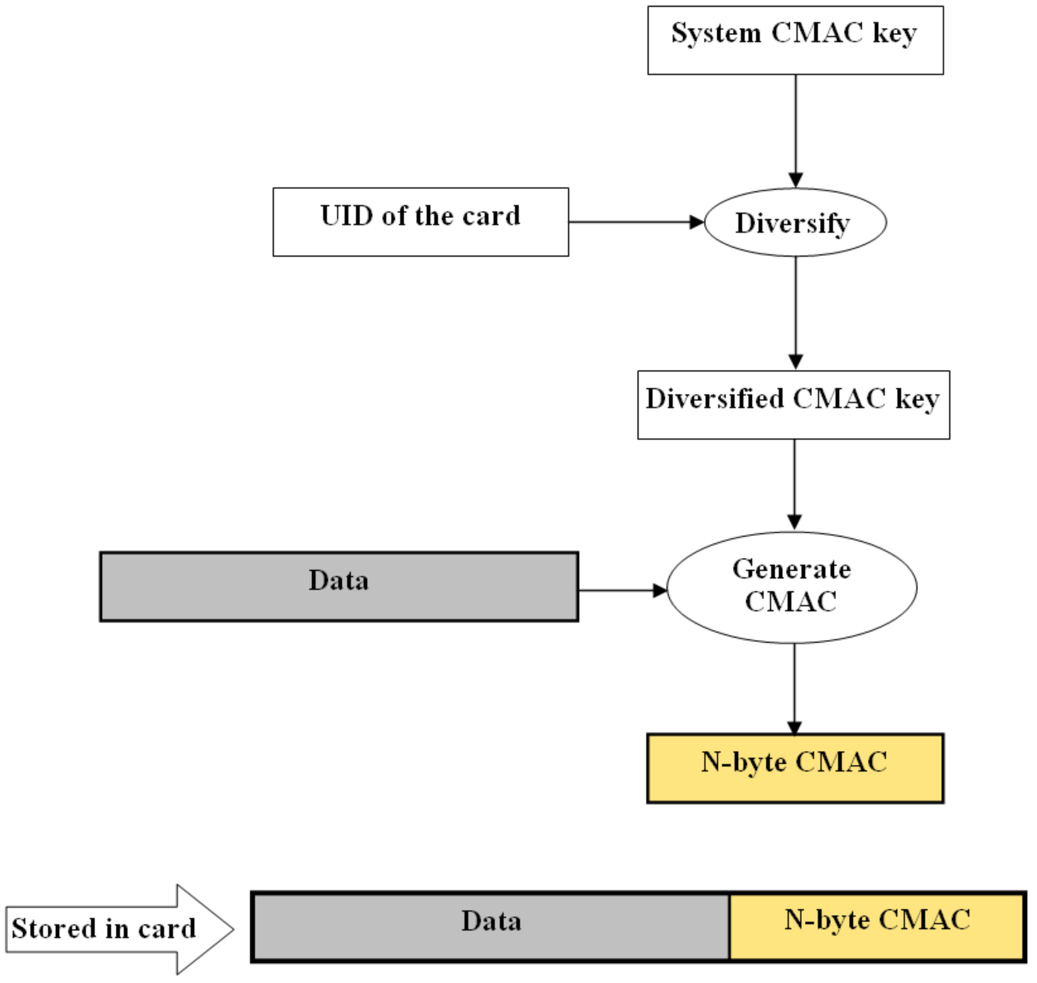

Figure 4. Calculating of SEAL for storage data

Figure 5 shows a widely used way of encryption of the data.

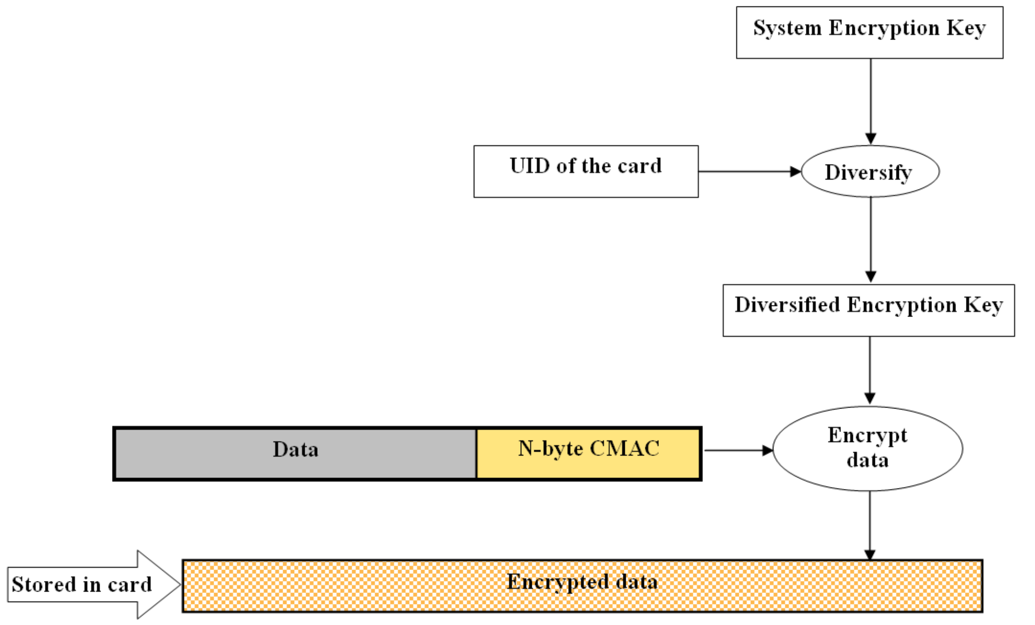

Figure 5. Encryption of data to be stored

2.4.1 Example of using General Purpose Cryptography in applications

In the following example logical channel 2 and 3 have been used for off-line crypto calculation. Other channels can be used to other purposes e.g. card authentication.

Table 9. Example of using general purpose cryptography in applications

step	Indication		Data / Message	Comment
Activating the System CMAC Key in logical channel 2, Key entry nr. 7 and version 01.				
1	SAM_ ActivateOfflineKey C-APDU	>	8201010009070104708A97562080	P1 = 01; key diversification. Data field is the SAM key entry number, version number and DivInp (UID).
2	SAM_ ActivateOfflineKey R-APDU	<	9000	The key entry number 7 with version 01 is ready for off-line crypto calculation.
Activating the System encryption Key in logical channel 3, Key entry nr. 8 and version 02.				
3	SAM_ ActivateOfflineKey C-APDU	>	8301010009080204708A97562080	P1 = 01; key diversification. Data field is the SAM key entry number, version number and DivInp (UID).
4	SAM_ ActivateOfflineKey R-APDU	<	9000	The key entry number 8 with version 02 is ready for off-line crypto calculation.
Now preparing the cryptogram				
5	Application data	=	3C4162752049736D61696C3E	12-byte data.
6	UID of the card	=	04708A97562080	7-byte UID of the detected card.
7	SAM_Generate_ MAC C-APDU	>	827C00040C3C4162752049736D61696C3E00	P2 = the CMAC length (here 04), Data field is the application data.

step	Indication		Data / Message	Comment
8	SAM_Generate_MAC R-APDU	<	902A0A769000	4-byte CMAC+ SW1SW2
9	Application data with CMAC	=	3C4162752049736D61696C3E902A0A76	12-byte application data and CMAC as shown in Figure 4 .
10	SAM_EncipherOffline_Data C-APDU	>	830E0000103C4162752049736D61696C3E902A0A7600	Data field is the plain text (multiple block size).
11	SAM_EncipherOffline_Data R-APDU	<	234D10C555B57C1D8E46180019D876F49000	Encrypted data + SW1SW2
12	Encrypted data to store	=	234D10C555B57C1D8E46180019D876F4	16-bytes encrypted data to store in the card as shown in Figure 5

Step 7 to 12 can be repeated as many times, they required. The keys are active as long the logical channels are not deactivated or used for other authentications.

3 PKI – Public Cryptography Infrastructure

3.1 RSA

The MIFARE SAM AV3 supports RSA Key generation, export and import Key entries, Signature generation and verification. Also, RSA encryption and decryption is possible.

3.1.1 Create RSA Key Pair

step	Indication		Data / Message	Comment
1	PKI_ GenerateKeyPair APDU	>	801501000E 01 0043 0000FF 0040 0004 00010001	This command creates RSA-512 bit, Private Key Export is allowed, CRT used on Key number 0x01
2	Status	<	9000	Return of SAM AV3

As a public exponent PKI_e, the 5th Fermat number 2^{16}+1(=0x00010001) is chosen, which is usual for RSA

This command will take 10 to 15 seconds to execute.

After that, you will be able to use the Key for generation and verification of signatures or for en/decryption.

3.1.2 Export Public Key

The public Key can be exported via the following command

step	Indication		Data / Message	Comment
1	PKI_Export Public Key APDU	>	8018010000	Export Public Key from pos 0x01
2	Return of data	<	0043 0000FF 0040 0004 **81 C2F594423923E85F3AF5A F439971FE0DF3BFD8013F 6BE57E553B87581DAA5C 2E0D1F4FC4145489AF295 4E5512553FE8E7974E5B0 C90B61FD94E677FBDA17 D5** 00010001 9000	Return of the public Key SET || CEK || V_CEK || PKI_NLen || PKI_eLen || PKI N (Public Key) || PKI_e || 9000

This key and the public exponent PKI_e can be shared with anyone to verify signatures created with this key.

3.1.3 Sign data

As a next step, we want to sign some data with the generated Key.

The message we want to sign is 0xCCAAFFEE

The algorithm for signing should be SHA-1

step	Indication		Data / Message	Comment
1	PKI_ GenerateHash APDU	>	8017000008 00000004 CCAAFFEE 00	Generate a Hash with SHA-1 of the message. 00000004 is the message length in Bytes
2	Return of data	<	0BDA3BAB6E3551F5B4 6C24DBBB92EDC9DEA 1588C 9000	Hash
3	PKI_ GenerateSignature	>	8016000015 01 0BDA3BAB6E3551F5B4 6C24DBBB92EDC9DEA 1588C	Generates the RSA Signature of the given Hash with the given PKI Key number
4	Return status	<	9000	SAM AV3 succeeded to create the signature
5	PHI_ SendSignature	>	801A000000	Retrieves the Signature from the SAM AV3 using the SendSignature command
6	Signature	<	4A5B63F6CD2EEE6F2B EF69E40669A7E0D190D 43761A4A69103BF07A2 889857F4AAA358DB968 E826A3C475006FD7FC5 CC57A9CEF50C091844 A0C710201ECBA7CD 9000	RSA Signature || Status

3.1.4 Verify the Signature

step	Indication		Data / Message	Comment
1	PKI_ VerifySignature	>	801B0000 01 0BDA3BAB6E3551F5B4 6C24DBBB92EDC9DEA 1588C 4A5B63F6CD2EEE6F2B EF69E40669A7E0D190D 43761A4A69103BF07A2 889857F4AAA358DB968 E826A3C475006FD7FC5 CC57A9CEF50C091844 A0C710201ECBA7CD	Verifies the hash and the signature
2	Return status	<	9000	Verification of the given signature with the Hash and given key has passed

3.2 ECC

ECC is used for example in MIFARE Classic EV1, or MIFARE PLUS EV1 products as originality signature. The following example shows how to verifiy the signature of a MIFARE PLUS EV1

3.2.1 Verify MIFARE originality signature

step	Indication		Data / Message	Comment
1	PKI_ ImportEccKey	>	8021000043 000000FE00FFFE001C00044409ADC42F91A839 4066BA83D872FB1D168 03734E911170412DDF8 BAD1A4DADFD0416291 AFE1C748253925DA39A 5F39A1C557FFACD34C 62E	Imports the public Key of MIFARE PLUS EV1 into the ECC Keystore. KeyNo = 0x00, SET=0x0000,ECC_ KeyNoCEK=0xFE, ECC_ KeyVCEK=0x00, no KUC, free access.
2	Return status	<	9000	
3	PKI_ ImportEccCurve	<	80220000 AD 00FE001C1CFFFFFFFF FFFFFFFFFFFFFFFFFF FFFFFF00000000000000 0000000001FFFFFFFF FFFFFFFFFFFFFFFFFF FFFFEFFFFFFFFFFFFF FFFFFFFFFFEB4050A85 0C04B3ABF5413256504 4B0B7D7BFD8BA270B3 9432355FFB4B70E0CBD 6BB4BF7F321390B94A0 3C1D356C21122343280 D6115C1D21BD376388B 5F723FB4C22DFE6CD4 375A05A07476444D581 9985007E34FFFFFFFF FFFFFFFFFFFFFFFFFF F16A2E0B8F03E13DD29 455C5C2A3D	Imports the ECC curve used in MIFARE PLUS EV1 secp224r1.
4	Return Status	<	9000	
5	PKI_ VerifyEccSignature	>	802000003F 0000 04 33086B60 389B164A5FD1A652FC6 D814753696FF5A68270 943DCE2A3B7D26F26D D6F3DB07C1AE3FEE02 A40AA5D444DA40BFC6 843C886DF983F47D048A	Verifies the Signature of a MIFARE PLUS EV1. The message to verify is the UID, in that case 4 byte.
6	Return status	<	9000	

4 References

1. **Data sheet –** Data sheet of MIFARE SAM AV3, document number DS3235xx.
2. **System guidance manual – MF4SAM30 (MIFARE SAM AV3)**, document number xx.
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** – **AN5212 – MIFARE SAM AV3 - Key Management and Personalization**, document number 5212xx.
5. **Application note – Symmetric Key Diversifications**, document number AN1653xx.
6. **Application note – AN5217 – MIFARE SAM AV3 for MIFARE Classic,** document number 5217xx.
7. **Application note – AN12704 – MIFARE SAM AV3 Host communication,** document number 5213xx, https://www.nxp.com/docs/en/application-note/AN12704.pdf.
8. **Application note – MIFARE SAM AV3 – For General Purpose Cryptography,** document number AN4462xx.

5 Legal information

5.1 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.

5.2 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.

5.3 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.

5.4 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: 7 July 2020
Document identifier: AN12702
Document number: 522111