# AN13762

## Using MIFARE SAM AV3 for NTAG 22x authentication and SUN verification

Rev. 1.0 — 7 November 2022 Application note

**Document information**

| Information | Content |
|---|---|
| Keywords | MIFARE SAM AV3, NTAG 224 DNA, SUN, SDM, CMAC, verification, authentication |
| Abstract | This application note shows how to use MIFARE SAM AV3 with NTAG 22x DNA for SUN verification and authentication. |

# Revision history

**Revision history**

| Rev | Date | Description |
|---|---|---|
| v.1.0 | 20221107 | Initial version |

# 1 Introduction

MIFARE SAM AV3 ([3]) is a secure element designed to work with MIFARE products like MIFARE DESFire or MIFARE Plus.

As NTAG DNA products use similar crypto functionalities as MIFARE products, MIFARE SAM AV3 can also be used together with NTAG 22x DNA ([1], [2]) for authentication and SUN message verification.

This application note covers the usage of MIFARE SAM AV3 specifically together with NTAG22x DNA products, NTAG 424 DNA is covered in a separate application note [4].

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

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.

## 2 Creating a SAM key entry for usage with NTAG 22x DNA

To support the authentication and SUN message verification, the secret key to be used needs to be injected into the MIFARE SAM AV3 symmetric keystore. This key can be used either diversified or non-diversified.

NTAG 22x DNA 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 NTAG 22x DNA is not natively implemented in MIFARE SAM AV3.

The following example writes an all 00s AES-128 key entry into MIFARE SAM AV3 at KeyEntry 0x01:

**Table 1. Preparing the KeyEntries for use with NTAG 22x DNA**

| Step | Command | Direction | Message | Comment |
|---|---|---|---|---|
| 1 | SAM_ChangeKey Entry | > | 80C101FF40<br>00000000000000000000000000000000<br>00000000000000000000000000000000<br>00000000000000000000000000000000<br>000000000000FF20000000000400<br>FEFE | Inject an AES128 all 00s (default key) key into SAM KeyEntry 0x00. KeyClass is OfflineCrypto, KeyVAEK is set to 0xFE, this means that this key can subsequently be used without Host Authentication on MIFARE SAM AV3. For details refer to [3]. |
| 2 | Response | < | 9000 | Success |

# 3 Downloading a key from MIFARE SAM AV3 to NTAG 22x DNA

As the NTAG 22x DNA 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 an NTAG 22x DNA, the key needs to be dumped from the SAM and written into the corresponding memory area in NTAG 22x DNA.

To be able to dump a secret key from MIFARE SAM AV3, the KeyEntry needs to have bit 3 of the ExtSET bytes enabled. This makes 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 2. Secure messaging example**

| Step | Command | Direction | Message | comment |
|---|---|---|---|---|
| **dump plain** | | | | |
| 1 | SAM_ChangeKey Entry | > | 80C101FF40<br>00000000000000000000000000000000<br>00000000000000000000000000000000<br>00000000000000000000000000000000<br>000000000000<br>FF200000010209000000 | 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_DumpSecret Key | > | 80D6000002010000 | Dump the secret key in plain |
| 4 | Key Data | < | 00000000000000000000000000000000<br>9000 | Secret key and status code |
| **dump diversified** | | | | |
| 5 | SAM_ChangeKey Entry | > | 80C101FF40<br>00000000000000000000000000000000<br>00000000000000000000000000000000<br>00000000000000000000000000000000<br>000000000000<br>FF200000010219000000 | Load Key into KeyEntry 0x01 of MIFARE SAM AV3. ExtSet bit 3 and bit 4 are enabled, dump of secret key is allowed but only in diversified form (ExtSet = 0x0019) |
| 6 | Success | < | 9000 | |
| 7 | SAM_DumpSecret Key | > | 80D6020009010004112233445566 00 | Dump the secret key in plain, diversified form (P1 = 0x02), div input = 04112233445566 |
| 8 | Key Data | < | 2360D14689E17C7AA9821665E68<br>A0099<br>9000 | Diversified secret key and status code |

The dumped key needs to be written inside the AES Key_x area inside the NTAG 22x DNA memory. This process is described in the data sheets [1] and [2].

# 4 Authenticating NTAG 224 DNA

There is no dedicated command for Authenticating NTAG 224 DNA on MIFARE SAM AV3 available. Therefore, authentication is done "by hand" using the offline crypto functionalities on MIFARE SAM AV3. There is no AES-128 authentication available on NTAG 22**3** DNA.

**Table 3. Authenticating NTAG 224 DNA**

| 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 NTAG 224 DNA |
| 4 | E(Kx,RndB) | < | AF37B7F49CD707F8D8E29 DDEC256912187 | 0xAF + E(Kx,RndB) |
| 5 | LoadIV | > | 8071000010 00000000000000000000000000000000 | Sets the SAM's IV to all 0x00s |
| 6 | Response | < | 9000 | success |
| 7 | SAM_Decipher Offline_Data | > | 800D00001037B7F49CD707F8D8E29 DDEC25691218700 | Decrypts the encrypted RndB |
| 8 | RndB | < | D220B067DE955EFA0A24623F4F216 AC59000 | RndB |
| 9 | GetRandom | > | 8084000010 | Generates 16 byte random data as RndA |
| 10 | RndA | < | 07F8AAE1B62FB3930977BDCD16157 E8B9000 | RndA |
| 11 | LoadIV | > | 8071000010 00000000000000000000000000000000 | Sets the SAM's IV to all 0x00s |
| 12 | Response | < | 9000 | success |
| 13 | SAM_Encipher Offline_Data | > | 800E00002007F8AAE1B62FB3930977 BDCD16157E8B20B067DE955EFA0 A24623F4F216AC5D200 | Encrypts the concatenation of RndA and RndB' (RndB' is the rotation of RndB by one byte) |
| 14 | E(Kx,RndA\|\|RndB') | < | 66FDB31BFD79F3C02E17C44 FCDB7466B669DFA2F986F568725703 DDF47D0243D9000 | Encrypted RndA \|\| RndB' |
| 15 | Authenticate part 2 | > | AF66FDB31BFD79F3C02E17C44 FCDB7466B669DFA2F986F568725703 DDF47D0243D | Authenticate part 2 sent to NTAG 224 DNA |
| 16 | E(Kx,RndA') | < | 002D9194C800DBA0C4B8A85 CACD54F6568 | 0x00 (success) and encrypted RndA' |
| 17 | LoadIV | > | 8071000010 00000000000000000000000000000000 | Sets the SAM's IV to all 0x00s |
| 18 | Response | < | 9000 | success |
| 19 | SAM_Decipher Offline_Data | > | 800D0000102D9194C800DBA0C4B8 A85CACD54F656800 | Decrypts the encrypted RndA' |

**Table 3. Authenticating NTAG 224 DNA***...continued*

| Step | Command | Direction | Message | Comment |
|---|---|---|---|---|
| 20 | RndA' | < | F8AAE1B62FB3930977BDCD16157E8B079000 | RndA' |

# 5 SUN message verification

For SUN message verification, the same key settings in MIFARE SAM AV3 are required as for authentication.

First of all, the SUN message needs to be read from the NTAG 22x DNA. This can be done in several ways, either the message is conveyed as NDEF content, or the memory is read with a READ command at the position where the mirroring is pointing to. After this, the SUN part needs to be converted back into hex data from the ASCII representation, and can be sent to the MIFARE SAM AV3 for verification.

The SUN message is always a concatenation of the UID (14 byte ASCII), the NFC_CTR (6 byte ASCII) and the CMAC (16 byte ASCII), separated by an "x" (0x78) character. The total length is 39 bytes (ASCII).

**Table 4. Authenticating NTAG 224 DNA**

| Step | Command | Direction | Message | Comment |
|---|---|---|---|---|
| 1 | Read page 0x39 | > | 3039 | read configuration page to obtain mirror location |
| 2 | content of page 0x39 - 0x3C | < | **80**00**09**4<br>C900000000000000000000000 | CFG_B0 → 0x80: Mirroring enabled, MIRROR_BYTE = 00b. MIRROR_PAGE → 0x09 |
| 3 | FastRead page 0x09 until 0x13 | > | 3A0913 | read pages 0x09(MIRROR_PAGE) until page 0x13 (MIRROR_PAGE + 10). This will result in 44 bytes of data. The SUN message is always 39 bytes long (ASCII), hence this command will for sure cover the whole SUN message |
| 4 | SUN message in ASCII read out of the memory | < | 30344234424634413033313039307830<br>30303030357832463544373630363534<br>45393141344200003030303 0 | SUN message in ASCII representation |
| 5 | UID (ASCII) | = | 30344234424634413033313039 30 | |
| 6 | UID (hex) | = | 04B4BF4A031090 | |
| 7 | NFC_CTR (ASCII) | = | 303030303035 | |
| 8 | NFC_CTR (hex) | = | 000005 | |
| 9 | CMAC (ASCII) | = | 32463544373630363534453931413442 | |
| 10 | CMAC (hex) | = | 2F5D760654E91A4B | |
| 11 | ActivateOffline Key | > | 80010000020100 | Activate the secret key |
| 12 | Response | < | 9000 | success |
| 13 | SAM_GenerateMAC | > | 807C00800A04B4BF4<br>A03109000000500 | Generate CMAC over UID and NFC_CTR in hex values |
| 14 | SAM Response | < | 2F5D760654E91A4B9000 | CMAC + success code |
| 15 | compare CMACs | = | 2F5D760654E91A4B = 2F5D760654<br>E91A4B | SUN Message verified |

In case the message is retrieved via NDEF, steps 1 to 4 are a bit different, but from step 5 onwards the process is the same. For above example, the NDEF message would look like this: "nxp.com/data=04B4BF4A031090x000005x2F5D760654E91A4B". This

message already contains UID, NFC_CTR and CMAC, which can be used for the verification.

The necessary steps to set up the SUN feature are described in [1] and [2].

# 6 Abbreviations

**Table 5. Abbreviations**

| Acronym | Description |
|---|---|
| AES | Advanced Encryption Standard |
| NDEF | NFC Data Exchange Format |
| NFC | Near Field Communication |
| SAM | Secure Application Module |
| SE | Secure Element |
| SUN | Secure Unique NDEF |

# 7 References

[1] **Data sheet NTAG 224 DNA** - NT2H2421G0 NTAG 224 DNA - NFC T2T compliant IC

[2] **Data sheet NTAG 224 DNA** - NT2H2421G0 NTAG 223 DNA - NFC T2T compliant IC

[3] **Data sheet MIFARE SAM AV3** - DS3235xx - available via Secure Files on NXP.com

[4] **Application note** - AN12697 MIFARE SAM AV3 for NTAG 424 DNA

# 8 Legal information

## 8.1 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.

## 8.2 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.

**Terms and conditions of commercial sale** — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

**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.

## 8.3 Licenses

**Purchase of NXP ICs with NFC technology** — Purchase of an NXP Semiconductors IC that complies with one of the Near Field Communication (NFC) standards ISO/IEC 18092 and ISO/IEC 21481 does not convey an implied license under any patent right infringed by implementation of any of those standards. Purchase of NXP Semiconductors IC does not include a license to any NXP patent (or other IP right) covering combinations of those products with other products, whether hardware or software.

## 8.4 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 Plus** — is a trademark of NXP B.V.

**NTAG** — is a trademark of NXP B.V.

# Tables

# Contents





For more information, please visit: http://www.nxp.com

Date of release: 7 November 2022
Document identifier: AN13762