AN12698

MIFARE SAM AV3 for NTAG 5, ICODE DNA and UCODE DNA

Rev. 1.2 — 12 March 2020 Application note
522012 COMPANY PUBLIC

Document information

Information	Content
Keywords	MIFARE SAM AV3, ICODE, UCODE, DNA, TAM Authenticate, MF4SAM3, NTAG 5, MAM Authenticate
Abstract	This application note shows the use of MIFARE SAM AV3 in combination with NTAG 5, ICODE DNA and UCODE DNA

Revision history

Rev	Date	Description
1.2	20200310	Added NTAG 5 link and NTAG 5 boost
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 5 link, NTAG 5 boost (both referred to NTAG 5 in this document), ICODE DNA and UCODE DNA. In this document, the SAM is used in S mode. 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 [1].

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 [2].

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

1.2 Abbreviations

Refer to application note “AN5210 MIFARE SAM AV3 – Quick Start up Guide” [1].

1.3 Examples presented in this document

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

= Preparation of data by SAM, PICC or host.

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

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

C-APDU:

CLA	INS	P1	P2	Lc	Data (nc)	Le

R-APDU:

Response data	SW1	SW2

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

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

1.4 S interface

The host is managing the communication to SAM AV3 and NTAG 5 / ICODE / UCODE via the RF Controller.

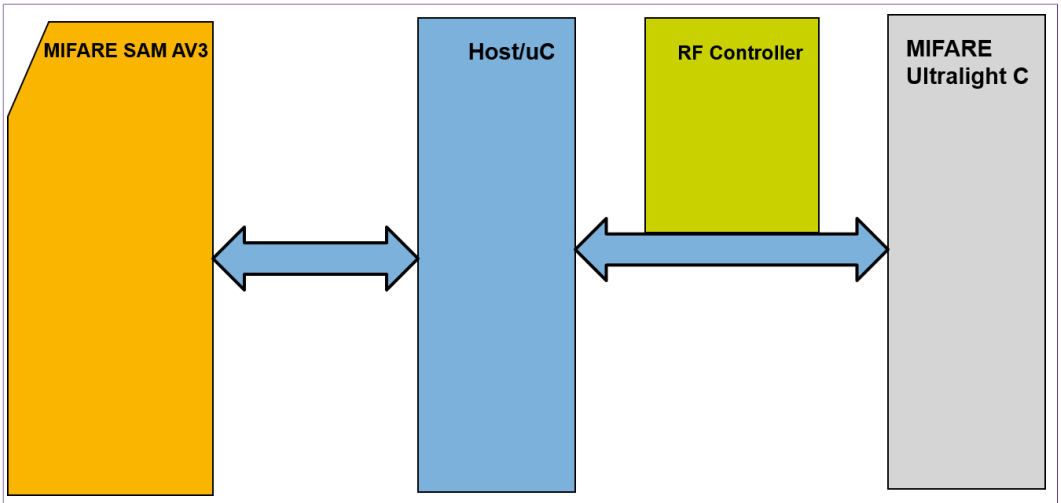


Figure 1. Architecture in non-X interface

2 NTAG 5, ICODE DNA and UCODE DNA

MIFARE SAM AV3 can be used to perform the AES authentication for NTAG 5, ICODE DNA and UCODE DNA. Both, tag authentication and mutual authentication are available. More details about these functionalities can be found in the product datasheets of NTAG 5, ICODE DNA and UCODE DNA [3,4,5].

For NTAG 5, ICODE and UCODE, only **S-mode** support is available.

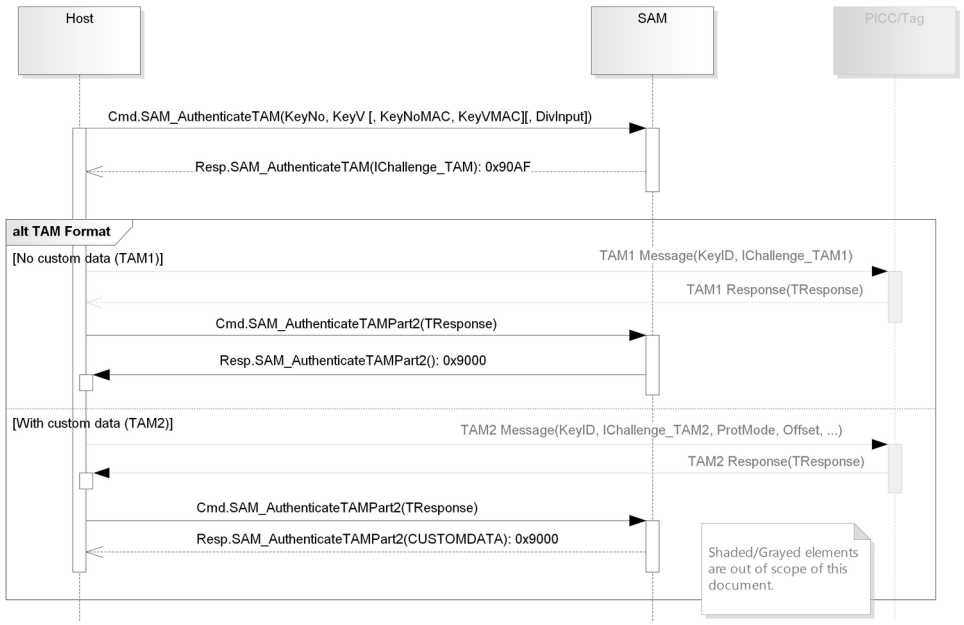
The following example for TAM is valid for NTAG 5, ICODE DNA and UCODE DNA.

The following example for MAM is valid for NTAG 5 and ICODE DNA.

2.1 Authenticate TAM

In this example, a TAM authentication is performed. The TAM sequence looks like the following:

Figure 2. TAM Authenticate sequence



The command uses one AES-128 Key from the Keystore to perform the authentication.

To perform this example, a key with the following attributes needs to be created:

- KeyType = AES128
- KeyClass = PICC
- KeyNoCEK = 0x00 and KeyVCEK = 0x00
- RefNo. KUC = 0xFF (no KUC used)
- KeyNoAEK = 0x00 and KeyVAEK = 0x00
- Diversified use only: This property is not set in this example, however it is strongly recommended to set for real applications. This setting prohibits the use the key in an undiversified form.

- Key Value: 0x00000000000000000000000000000000, Version 0x01
  The KeyID on the tag is 0x00 in this example.

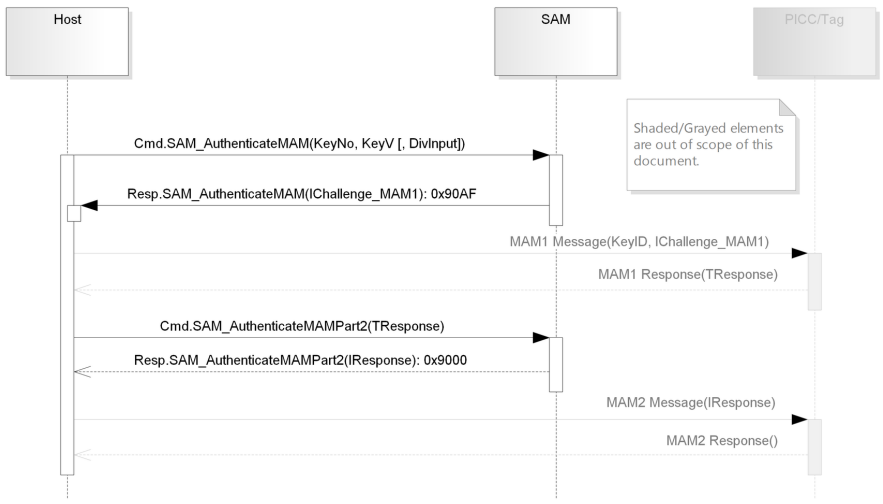
Table 1. Example - SAM_AuthenticateTAM

step	Indication		Data / Message	Comment
1	Request IChallenge_ TAM from SAM	>	80B0000002090100	Use Key 0x09 version 0x01
2	Receive IChallenge_ TAM from SAM	<	A2E61C15CF69D1F3BC 2890AF	The SAM AV3 answers with 10 Byte random challenge and SW1SW2 as 0x90AF
3	Send IChallenge_TAM to NTAG 5/ICODE DNA/UCODE DNA	>	3500000028BCF3D169C F151CE6A2	Pass the received IChallenge along with the Authenticate command to the NTAG 5/ICODE DNA/UCODE DNA. **Attention**: The byte order is reversed!
4	Receive TResponse from NTAG 5/ICODE DNA/UCODE DNA	<	A7C76124B0CAC5B66FF E3BA594D838C2DF	The NTAG 5/ICODE DNA/UCODE DNA answers with A7 and the TResponse
5	Send TResponse to SAM AV3	>	80B0000010DFC238D89 4A53BFE6FB6C5CAB02 461C7	Pass the TResponse without the A7 **Attention**: The byte order is reversed.
6	Return Code	<	9000	Return code from SAM signalizing the TAM is pass.

2.2 Authenticate MAM

In this example, a MAM authentication (mutual authentication) is performed. This example is only valid for NTAG 5 / ICODE DNA. The MAM sequence looks like the following:

Figure 3. TAM Authenticate sequence



The command uses one AES-128 Key from the Keystore to perform the authentication.

To perform this example, a key with the following attributes needs to be created:

- KeyType = AES128
- KeyClass = PICC
- KeyNoCEK = 0x00 and KeyVCEK = 0x00
- RefNo. KUC = 0xFF (no KUC used)
- KeyNoAEK = 0x00 and KeyVAEK = 0x00
- Diversified use only: This property is not set in this example, however it is strongly recommended to set for real applications. This setting prohibits the use the key in an undiversified form.
- Key Value: 0x11111111111111111111111111111111, Version 0x02
  The KeyID on the tag is 0x01 in this example.

Table 2. Example - SAM_AuthenticateMAM

step	Indication		Data / Message	Comment
1	Request IChallenge_ MAM from SAM	>	80B2000002090200	Use Key 0x09 version 0x02
2	Receive IChallenge_ MAM from SAM	<	2AAF36011365224B134A90AF	The SAM AV3 answers with 10 Byte random challenge and SW1SW2 as 0x90AF
3	Send IChallenge_ MAM to NTAG 5/ ICODE DNA	>	3500020 14A134B2265130136AF2A	Pass the received IChallenge along with the Authenticate command to the NTAG 5/ ICODE DNA **Attention**: The byte order is reversed!
4	Receive TResponse from NTAG 5/ ICODE DNA	<	A74C76F7D4458E1C520C30798F7D73B24BC522F47D10C4	The NTAG 5/ ICODE DNA answers with A7 and the TResponse
5	Send TResponse to SAM AV3	>	80B2000016C4107DF422C54BB2737D8F79300C521C8E45D4F7764C00	Pass the TResponse without the A7 **Attention**: The byte order is reversed.
6	Receive IResponse from SAM AV3	<	84D8EF30D3581C2561A26330A6ABFECD9000	The SAM AV3 answers with 16 Byte IResponse and 0x9000
7	Send IResponse to NTAG 5/ ICODE DNA	>	350006CDFEABA63063A261251C58D330EFD884	Pass the IResponse to the NTAG 5/ ICODE DNA. **Attention**: The byte order is reversed.
8	Receive return code from NTAG 5/ ICODE DNA	<	A7	NTAG 5/ ICODE DNA responds with A7 to signalize the authentication is pass

3 References

1. **Application note** – **AN12695 – MIFARE SAM AV3 – Quick Start up Guide**, document number 5210xx, https://www.nxp.com/docs/en/application-note/AN12695.pdf.
2. **Data sheet –** Data sheet of MIFARE SAM AV3, document number 3235xx.
3. **Data sheet –** Data sheet of UCODE DNA, document number 3201xx.
4. **Data sheet –** Data sheet of ICODE DNA, document number 3486xx.
5. **Data sheet –** Data sheet of NTA5332, document number 5447xx.

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.

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.

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.

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: 12 March 2020
Document identifier: AN12698
Document number: 522012