AN10975

MIFARE SAM AV2 Documentation and Sampling

Rev. 2.3 — 2 November 2011
198623

Application note
COMPANY PUBLIC

Document information

Info	Content
Keywords	MIFARE SAM AV2, Secure Key Storage, DES, TDEA, AES, RSA. Key Usage Counters.
Abstract	This application note introduces MIFARE SAM AV2 and all documentation and samples.

Revision history

Rev	Date	Description
2.3	20111102	Table updated in Section 2.6 MIFARE SAM AV2 samples
2.2	20111010	Table updated in Section 2.6 MIFARE SAM AV2 samples
2.1	20110721	Ref. 7 updated in Fig 2
2.0	20100915	BU-ID document number changed, no content change
1.0	20100901	Initial version.

Contact information

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

For sales office addresses, please send an email to: salesaddresses@nxp.com

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 the information on all the available support items for application development using MIFARE SAM AV2.

1. 1. MIFARE Ultralight C, MIFARE Classic, MIFARE Plus, MIFARE DESFire, MIFARE DESFire EV1

1.2 Abbreviations

These abbreviations are used in all the MIFARE SAM AV2 application notes.

Table 1. Abbreviations

Abbreviation	Meaning
AID	Application ID
APDU	Application Protocol Data Unit
API	Application Programming Interface
ATR	Answer To Reset
ATS	Answer To Select
C-APDU	Command APDU
CBC	Cipher-Block Chaining
CEK	Change Entry Key
CID	Card IDentifier
CLA	Class byte
CMAC	Cipher based MAC
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
DF	DESFire
FID	File ID
FSCI	Frame Size for proximity Card Integer
GPRS	General Packet Radio Service
HSM	Hardware Security Module
HVQFN32	Heatsink Very-thin Quad Flat-pack No-leads (32-pin)
INS	Instruction byte
IV	Init Vector
KST	Key Storage Table
KUC	Key Usage Counters
Lc	Length field for coding the Nc field
Le	Length filed for coding the Ne field
LFI	Last Frame Indicator

Abbreviation	Meaning
LRC	Longitudinal Redundancy Check
LRU	Latest Recently Used
LSB	Lowest Significant Byte
MAC	Message Authentication Code
MSB	Most Significant Byte
Nc	Number of bytes in the command data field
Ne	Number of bytes expected in the response data field
P1	Parameter 1
P2	Parameter 2
PCB	Protocol Control Byte
PCD	Proximity Coupling Device (reader/writer unit)
PCM	Product Contact Module
PC/SC	Personal Computer Smart Card
PICC	Proximity Integrated Circuit Card
POST	Point of Service Terminal
PPS	Protocol and Parameter Selection
R-APDU	Response APDU
RATS	Request for Answer To Select
RFU	Reserved for Future Use
SAK	Select AcKnowledge
SAM	Secure Application Module
SET	Setting
SIM	Subscriber Identification Module
SW	Status word
TDEA	Triple Data Encryption Algorithm
UID	Unique IDentification number
X -functions	The functions offered by SAM in direct connection to RC52X or PN51X using I2C.

2. MIFARE SAM AV2 Start up information

2.1 Introduction

Secure **A**pplication **M**odule (SAM) is a semiconductor where the cryptographic keys can be stored and used securely.

SAMs are available from NXP in the following formats:

- Contact-only module (PCM 1.1) as defined in ISO/IEC 7816-2 (figure a).
- HVQFN32.

The samples of SAM are delivered for your evaluation in SIM card format (ID-000) embedded in ID-1 size plastic card (figure b).

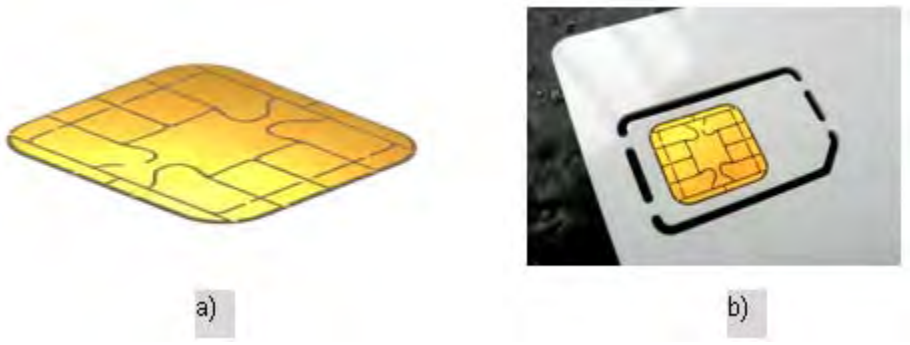

Fig 1. SAM contact module and SAM Card

The interface of SAM is ISO/IEC 7816-3 contact-only interface. It supports standard communication speed according to ISO/IEC 7816-3, protocol T =1, and also very high speed up to **1.5 Mbps**.

Although the SAMs can be seen as a contact smart card from the interface point of view, the SAMs do not allow creating or storing user data/file structure. SAMs offer moreover crypto capabilities as secret keys can be stored in the SAM securely and can be used for cryptographic functions in a secure way.

2.2 Available SAM

Currently, NXP's MIFARE SAM portfolio consists of three SAMs. Some of their features and their differences between versions are listed in the following table.

Table 2. Different SAMs

Features	MIFARE SAM AV1 (P5DF072EV2/ T0PD4090)	MIFARE SAM AV2 (P5DF081)
Communication Interface	ISO/IEC 7816, Class A, B, C. T = 1, up to 1.5 Mbps. I^2C interface to MFRC52X and PN51X.	ISO/IEC 7816, T = 1, up to 1.5 Mbps. Class A, B. I^2C interface to MFRC52X and PN51X.
Cryptographic Algorithms	TDEA 112-bit and 168-bit key, MIFARE Crypto1. AES-128 and AES-192.	TDEA 112-bit and 168-bit key, MIFARE Crypto1. AES-128 and AES-192. RSA-up to 2048-bit key.
Public Key Infrastructure (PKI)	-	Yes
Hash function	-	Yes, SHA -1, SHA -224 and SHA -256.
Supported Product's Cryptography	MIFARE Classic, MIFARE Ultralight C, MIFARE DESFire, MIFARE DESFire EV1.	MIFARE Classic, MIFARE Ultralight C, MIFARE Plus, MIFARE DESFire, MIFARE DESFire EV1.
Secure host communication	-	Yes
X- functionalities	Yes	Yes

2.3 MIFARE SAM AV2 Product Modes

MIFARE SAM AV2 offers two different modes:

- MIFARE SAM AV2 in AV1 mode and
- MIFARE SAM AV2 in AV2 mode.

Some of those features are explained in the following table:

Table 3. MIFARE SAM AV2 modes

Feature	MIFARE SAM AV2 in AV1 mode	MIFARE SAM AV2 in AV2 mode
PKI	Not available.	Available.
Host Authentication	Possible with all types of keys (except MIFARE Crypto1 keys), 3-pass mutual authentication.	Allowed only with AES-128 or AES-192 key type, 4-pass mutual authentication.
Host communication	Only CMACed in response or plain.	Configurable communication, plain, CMACed or encrypted in both directions.
Secure messaging	Only CMAC in response, if configured.	Extended to bi-directional CMAC and encryption mode, together with command counter.
Classification of symmetric Key entries	Not available.	Host, PICC, Offline change and Offline Crypto key.
Dumping Key	Secret key and session key can be dumped in the same way.	Secret key and session key are dumped using two different commands and restrictions based on key class type. Possible to restrict the secret key dump while dumping diversified ones.

AV2 mode is more secure than AV1 mode: it is strongly recommended to use MIFARE SAM AV2 in AV2 mode.

MIFARE SAM AV2 is delivered from NXP in AV1 mode.

2.3.1 Switching MIFARE SAM AV2 from AV1 to AV2 Mode

SAM_LockUnlock command is used to switch MIFARE SAM AV2 from AV1 mode to AV2 mode. SAM master key entry of type AES can be used for this switching. The commands and sequences of switching a virgin MIFARE SAM AV2 to AV2 mode are explained in [1].

2.4 SAM Distinction

The historical bytes of the SAM ATR tell the type of the product.

Table 4. Historical bytes of different SAM

SAM	Historical bytes	Characters corresponding ASCII
MIFARE SAM	6D69666172652053414D00000000	MIFARE SAM
MIFARE SAM AV1	4445534669726538205341 4D2D58	DESFire8 SAM-X [2]
MIFARE SAM AV2	4D494641524520506C75732053414D	MIFARE Plus SAM [3]

The response of the “Get Version” command gives all the detail information about the SAM, see also [1].

2. 2. Internal project name.
3. 3. Internal project name.

2.5 MIFARE SAM AV2 Product Support Package

There are several HW, SW and documents to support you for your MIFARE SAM AV2 application development, known as Product Support Package (PSP).

Nr.	Item Name	Type	Short Description	Ordering Information
1	MIFARE SAM AV2 Sample	Hardware	ID-000 size embedded in ID-1 plastic card	Can be requested through NXP local contact
2	Reference Hardware (DIK)	Hardware	HW, SW and documents	Can be requested through NXP local contact
3	Reference boards	Hardware	Boards with RC523, for evaluation X mode	Can be requested through NXP local contact
4	Product specification MIFARE SAM AV2	Document	MIFARE SAM AV2 Datasheet.	Document nr. 1645xx[4].
5	MIFARE SAM AV2 System Guidance Manual	Document	Guidance for secure MIFARE SAM AV2 usage.	Document nr. 1869xx.
6	Application notes	Document	Features and hints application notes	Document nr. 1821xx - 1830xx
7	MIFARE Reader Library	Lib	A C library/API, with source code in ANSI C	Document nr. 1717xx
8	MIFARE discover	Executable	A SW tool to evaluate MIFARE SAM AV2	Document nr. 1866xx
9	MIFARE discover user Manual	Document	Describing the usages of MIFARE discover	Document nr. 1867xx
10	Standard Customer training	Training	A full day training and hands-on workshop for the developers	Can be requested through NXP local contact

Fig 2. MIFARE SAM AV2 Product Support Package

Documents, Libraries and Executables are strictly confidential, therefore valid NDA is needed prior to request. They can be requested over e-mail from NXP-Docu-Control: nxp.docu-control@nxp.com. Kindly keep your local contact informed, whenever you request any item.

4. 4. xx stands for the version number, e.g. 165410 is version 1.0 of document 1654

2.6 MIFARE SAM AV2 samples

The following samples can be requested over your local representative from our secure sample desk service (psh.sampledesk.blid-development@nxp.com):

ID	Name	Delivery Type
9352 931 23118	P5DF081X0/T1AD2060	PCM
9352 931 21118	P5DF081HN/T1AD2060	HVQFN32
8222 640 90547	P5DF081X0/T1AD2060 CARD	White Card
9352 968 33151	P5DF081HN/T1AR1070	HVQFN32
9352 968 41118	P5DF081X0/T1AR1070	PCM
8222 640 90787	P5DF081X0/T1AR1070 CARD	White card

2.6.1 MIFARE SAM AV2 Application notes

Application notes have been published to explain the features of SAMs together with implementation hints and examples. There is a set of application notes for MIFARE SAM AV2, listed in the following table, each of them are describing specific features.

(Contact your NXP support engineer regarding the availability of the application notes).

Table 5. MIFARE SAM AV2 Application notes

Application note	Document number	Addressed features
MIFARE SAM AV2 – Quick Start up Guide.	1821xx	Introduction, detection of SAM type, starting with a PC/SC reader.
MIFARE SAM AV2 – Interface and architecture.	1822xx	Communication interfaces, logical channels, functional types[5], architectures, product modes[6], storage.
MIFARE SAM AV2 – Key Management and Personalization.	1823xx	Key management and personalization of MIFARE SAM AV2.
Symmetric Key Diversification	1653xx	The CMAC based key diversification algorithm supported by MIFARE SAM AV2.

5. 5. MIFARE SAM AV2 has two types of functionalities: non-X and X functions.
6. 6. MIFARE SAM AV2 offers two modes: MIFARE SAM AV2 in AV1 mode and MIFARE SAM AV2 in AV2 mode.

Application note	Document number	Addressed features
MIFARE SAM AV2 – Host Communication.	1824xx	Secure communication between host and MIFARE SAM AV2.
MIFARE SAM AV2 – For MIFARE Plus.	1825xx	Standard functionalities for MIFARE Plus.
MIFARE SAM AV2 – For MIFARE DESFire EV1.	1826xx	Standard functionalities for MIFARE DESFire EV1.
MIFARE SAM AV2 – For MIFARE Ultralight C.	1827xx	Standard functionalities for MIFARE Ultralight C.
MIFARE SAM AV2 – For MIFARE Classic.	1828xx	Standard functionalities for MIFARE Classic 1KB and MIFARE Classic 4KB.
MIFARE SAM AV2 – X functionalities.	1829xx	X functionalities.
MIFARE SAM AV2 – General purpose cryptography.	1830xx	How to use MIFARE SAM AV2 for general purpose standard cryptographic calculation.

These application notes are the supplementary documents to the MIFARE SAM AV2 product functional specification [1], read functional specification before using application notes.

3. References

[1] P5DF081 MIFARE SAM AV2 functional specification, document number 1645xx.

[2] MIFARE discover user manual, document number 1867xx.

[3] MIFARE SAM AV2 System Guidance Manual, document number 1869xx.

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.

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 accepts 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.

4.3 Trademarks

Notice: All referenced brands, product names, service names and trademarks are property of their respective owners.

MIFARE — 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.

DESFire — is a trademark of NXP B.V.

5. Contents

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

Date of release: 2 November 2011
198623
Document identifier: AN10975