AN10833

MIFARE type identification procedure

Rev. 3.8 — 10 January 2023 Application note

Document information

Information	Content
Keywords	MIFARE, NTAG, ISO/IEC 14443
Abstract	This document describes how to differentiate between the members of the MIFARE card IC family. ISO/IEC 14443-3 describes the initialization and anti-collision procedure, and ISO/IEC 14443-4 describes the protocol activation procedure. This document shows how to use these procedures to deliver the chip type information for all MIFARE ICs and implementations/emulations.

Revision history

Revision history

Rev	Date	Description
3.8	20230110	Correction of Figure 1 to the latest version
3.7	20210810	• Addition of newest generation • General restructuring with focus on the GetVersion command
3.6	20160711	Update for MIFARE Plus EV1
3.5	20140327	Update for multi-MIFARE implementation and implementation in UICC
3.4	20121029	Update for MIFARE implementation in a device
3.3	20110928	Update for TNP3xxx
3.2	20110829	Update for the new MIFARE Classic with 7 byte UID option
3.1	20090707	Correction of Table 12
3	20090518	Third release (supersedes AN MIFARE Interface Platform, Type Identification Procedure, Rev. 1.3, Nov. 2004)

1 Introduction

1.1 Terms and abbreviations

Table 1 shows the terms and abbreviation used in this document. All the “Type A” related definitions are used and described in the ISO/IEC 14443 documents.

Table 1. Abbreviations

Abbreviation	
ATQA	Answer To Request acc. to ISO/IEC 14443-4
ATS	Answer To Select acc. to ISO/IEC 14443-4
DIF	Dual Interface (cards)
COS	Card Operating System
CL	Cascade Level acc. to ISO/IEC 14443-3
CT	Cascade Tag, Type A
n.a.	not applicable
NFC	Near Field Communication
PCD	Proximity Coupling Device (“Contactless Reader”)
PICC	Proximity Integrated Circuit (“Contactless Card”)
PKE	Public Key Encryption (like RSA or ECC)
REQA	Request Command, Type A
SAK	Select Acknowledge, Type A
Select	Select Command, Type A
RID	Random ID, typically dynamically generated at Power-on Reset (UID0 = “0x08”, Random number in UID1… UID3)
RFU	Reserved for future use
UID	Unique Identifier, Type A
NUID	Non-Unique Identifier

In this document the term „MIFARE card“ refers to a contactless card using an IC out of the MIFARE Classic, MIFARE Plus; MIFARE DESFire or MIFARE Ultralight product family.

1.2 Scope

This document describes how to differentiate between the members of the MIFARE interface card IC family. The ISO/IEC 14443-3 describes the initialization and anti-collision procedure for type A, which delivers the card type information for all MIFARE cards.

The MIFARE cards are ISO/IEC 14443-3 compatible. Therefore already existing applications can easily be extended to operate with newer MIFARE chips respectively all other ISO/IEC 14443-3 compatible PICCs.

This document provides an easy guideline how the ISO/IEC 14443 compatible PCD should handle the MIFARE cards and how it can distinguish between the different available types of MIFARE cards.

1.3 MIFARE and ISO/IEC 14443

1.3.1 MIFARE

All MIFARE ICs are compliant to the ISO/IEC 14443 part 2 and part 3. The T=CL protocol as defined in the ISO/IEC 14443-4 is supported by MIFARE DESFire product family, the MIFARE Plus product family, and the NXP Dual or Triple Interface Card ICs (like SmartMX).

The MIFARE Classic with 1K memory, the MIFARE Classic with 4K memory, the MIFARE Ultralight EV1, the MIFARE Ultralight C, the MIFARE Plus, the MIFARE Plus EV1 and the MIFARE Plus EV2 (in security level 1 or 2) use the MIFARE Protocol (native command set) based on ISO/IEC 14443-3 only.

The MIFARE Classic with 1K memory, and the MIFARE Classic with 4K memory use the proprietary CRYPTO-1.

1.3.2 ISO/IEC 14443

The ISO/IEC 14443 consists of 4 parts.

1.3.2.1 Part 1: Physical characteristics

The ISO/IEC 14443-1 defines the physical size of the ISO/IEC 14443 PICC and its antenna.

1.3.2.2 Part 2: RF signal and power interface

The ISO/IEC 14443-2 defines the carrier frequency of 13.56 MHz, the modulation and coding, and the minimum and maximum field-strength. It is split up into type A (= MIFARE) and type B.

1.3.2.3 Part 3: Initialization and anti-collision

The ISO/IEC 14443-3 defines the start of communication and how to select the PICC. Sometimes this is called “Card Activation Sequence”. It is split up into type A (= MIFARE) and type B.

1.3.2.4 Part 4: Transmission protocol

The ISO/IEC 14443-4 defines the protocol for a data exchange between PCD and PICC. This protocol often is called “T=CL” protocol.

Please refer to the ISO/IEC 14443 documents for details.

2 Chip type identification procedure

2.1 Using GetVersion command to exactly identify the ICs

The MIFARE Ultralight EV1, MIFARE Plus EV1, MIFARE Plus EV2, MIFARE DESFire EV2, MIFARE DESFire EV3 and MIFARE DESFire Light support the command "GetVersion" to exactly identify the IC.

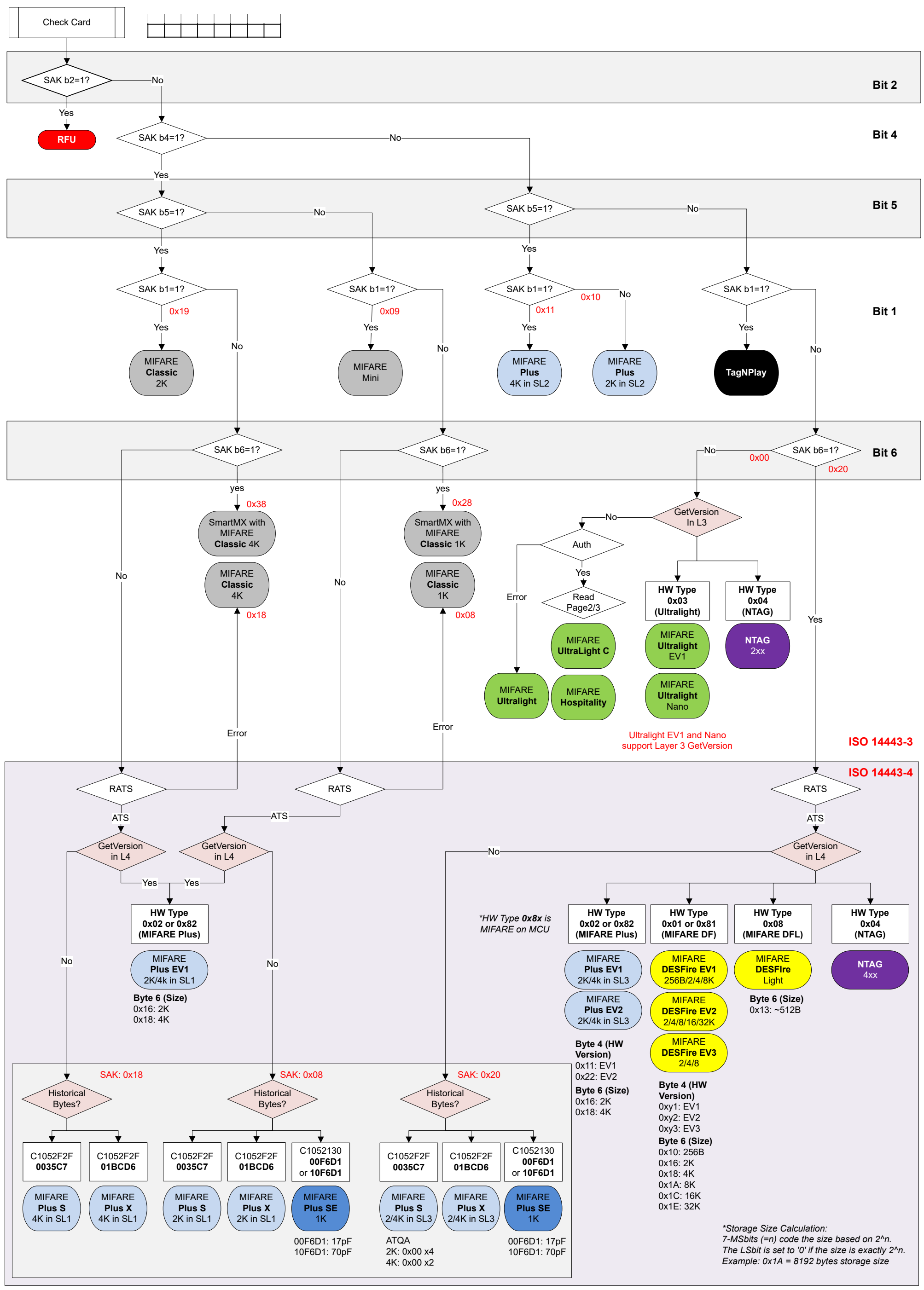
It is recommended to use only the GetVersion command to identify which IC Type currently is present on a reader.

The GetVersion command specification, as well as the GetVersion response can be found in the respective datasheets of the MIFARE products. In general, the lower nibble of the second byte of the GetVersion response gives the MIFARE product family, which is in many cases the most important information needed. The upper nibble defines if the device is a native MIFARE IC (0x0), an implementation (0x8), an applet on a Java Card (0x9) or MIFARE 2GO (0xA).

Table 2. GetVersion response byte 2 (HW/Product Type) meaning

Second Byte of GetVersion Response	Product
0xX1	MIFARE DESFire
0xX2	MIFARE Plus
0xX3	MIFARE Ultralight
0xX4	NTAG
0xX5	RFU
0xX6	RFU
0xX7	NTAG I^2C
0xX8	MIFARE DESFire Light

Below Figure 1 shows a flow diagram that can be used to distinguish all current MIFARE and NTAG products currently available using the GetVersion command, and for older generations the ATQA/SAK method.



MIFARE Plus SL0 is "Pre-Personalization" status, and not classified here.

1. This "Card Activation" requires a proper REQA/ATQA before the anti-collision Loop.
2. The bit numbering of the ISO/IEC 14443 starts with LSB = bit1!
3. The MIFARE Plus in Security Level 3 fully supports the ISO/IEC 14443-4.
4. SAK bit 2 is reserved for future use, i.e. bit 2 = 1 might give a different meaning to all other SAK bits.

Figure 1. MIFARE Card Activation examples*

* **Product-specific details can be found in the data sheet of the specific product**.

Note: It is not recommended to use the ATQA to determine card parameters due to possible collisions.

Note: The whole MIFARE Ultralight family uses the same ATQA and SAK.

Note: The MIFARE Plus in the SL3 uses the ATS or the card capabilities to distinguish between different card types.

Note: Only for older product generations, the following sections should be used for type identification. For MIFARE DESFire EV3 and MIFARE Plus EV2, the ATQA and SAK are configurable, so any ISO-conformal values are possible, therefore this cannot be used for type identification anymore.

2.2 Using the ISO activation parameters - not recommended!

Note: It is not recommended to use the ISO activation parameters for type identification.

The PCD typically polls for PICCs in the field. This is done with the REQA. When a PICC is within the operating range of the PCD and receives the REQA, any MIFARE PICC returns the ATQA.

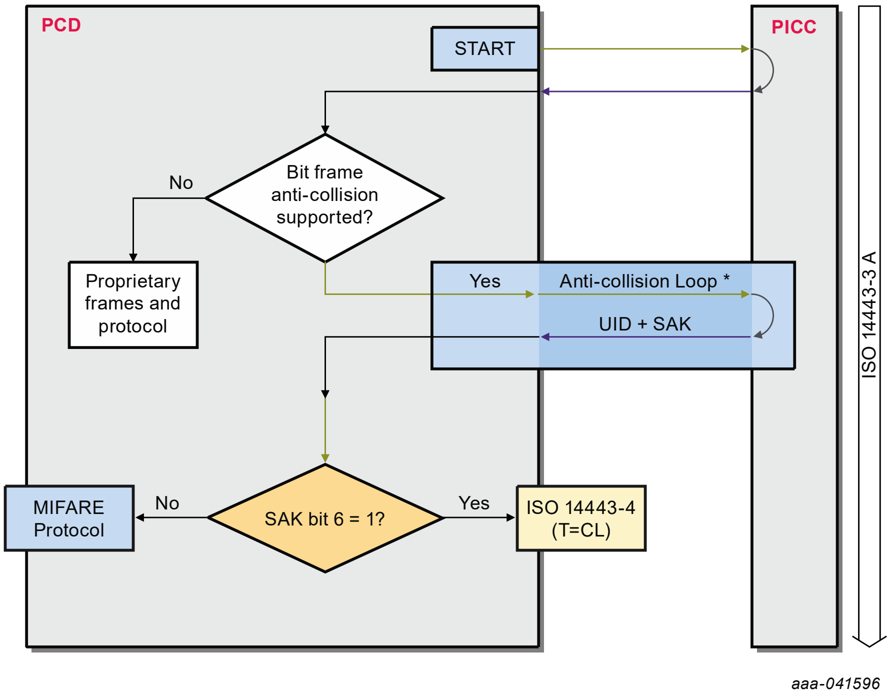
The content of the ATQA should be ignored in a real application, even though according to the ISO/IEC 14443 it indicates that the PICC supports the anti-collision scheme.

Note: In the case two or more MIFARE PICCs are in the operating field of the PCD at the same time, the received (combined) ATQA might contain “collisions”. That means there might be no unambiguous content anyway.

The complete card activation sequence is shown in the Figure 2 and Figure 3. The bit 6 [1] in the SAK indicates, whether the PICC is compliant to the ISO/IEC14443-4 or not. However, it does not necessarily indicate, whether the PICC supports the MIFARE Protocol or not. For more details about selecting the different type of MIFARE cards, refer to the Application note “AN10834 MIFARE ISO/IEC 14443 PICC Selection” (AN10834).

IMPORTANT NOTE: It is not advisable to use ATQA and SAK or any other protocol-related parameter to identify PICC's. If a system accepts or rejects PICC's based on protocol-related parameters rather than application-specific parameters (FCI / GetVersion / AID etc.), it may very well be that future technologies cannot be used in this system. On newer PICC generations, the activation parameters are already changeable, so a unique identification is anyhow not possible. In general, protocol and application data shall not be mixed at all. More recommendations on reader implementations can be found in [2]

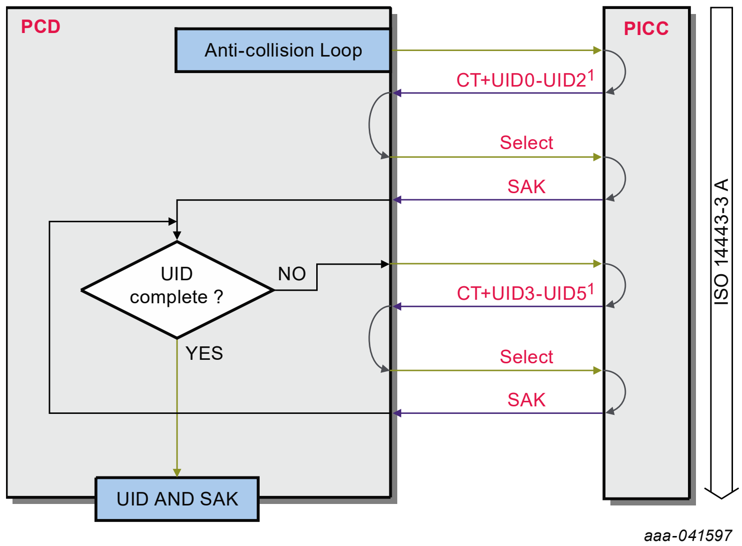
1 Attention: The bit numbering in the ISO/IEC 14443 document starts with bit 1 … 8, but not bit 0…7.



1. Details of the Anticollision Loop see Figure 3

Figure 2. Principle of the Card Activation Sequence

Note: For more details regarding the selection of one of the different types of MIFARE cards based on the SAK, refer to AN10834.



1. The CT (= Cascade Tag, Type A) byte indicates that the UID is not received completely yet. It indicates that another anti-collision loop on the next higher cascade level is required to get the complete UID.

Figure 3. Anticollision Loop as part of the Card Activation Sequence

2.3 Coding of Answer to Request Type A (ATQA)

Table 3 shows the coding of the ATQA as described in the ISO/IEC 14443-3. The RFU marked bits must be set to “0”, the proprietary bits might be used for proprietary codings. In real application, the content details of the ATQA are recommended to be ignored anyway.

Note 1: The bit numbering in the ISO/IEC 14443 starts with LSBit = bit 1, but not LSBit = bit 0. So one byte counts bit 1…8 instead of bit 0…7.

Note 2: The ISO/IEC 14443 transfers LSByte first. So e.g. 0x 00 44 (ATQA of the MF UL) is often received as 0x 44 00.

Table 3. ATQA Coding according to the ISO/IEC 14443-3

Bit number	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
ISO/IEC 14443-3	RFU				Proprietary				UIDsize		RFU	Bit Frame Anticollision				
Proprietary	0	0	0	0				1			0					
	0	0	0	0			1				0					
	0	0	0	0		1					0					
Single Size UID	0	0	0	0					0	0	0					
Double Size UID	0	0	0	0					0	1	0					
Triple Size UID	0	0	0	0					1	0	0					
RFU	0	0	0	0					1	1	0					
Anticollision supported	0	0	0	0							0	1	0	0	0	0
	0	0	0	0							0	0	1	0	0	0
	0	0	0	0							0	0	0	1	0	0
	0	0	0	0							0	0	0	0	1	0
	0	0	0	0							0	0	0	0	0	1

Table 4. ATQA Coding of NXP Contactless Card ICs which do not support a GetVersion command

X: depends on the COS

Bit number	Hex Value	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
ISO/IEC 14443-3		RFU				Proprietary				UID size		RFU	Bit Frame Anti-collision				
MIFARE Ultralight C	00 44	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0
MIFARE Classic EV1 1K	00 x4	0	0	0	0	0	0	0	0	0	x [1]	0	0	0	1	0	0
MIFARE Classic EV1 4K	00 x2	0	0	0	0	0	0	0	0	0	x [2]	0	0	0	0	1	0
MIFARE Plus 2K, SE(1K) (4 Byte NUID)	00 04	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0

Table 4. ATQA Coding of NXP Contactless Card ICs which do not support a GetVersion command*...continued*

X: depends on the COS

Bit number	Hex Value	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
MIFARE Plus 4K (4 Byte NUID)	00 02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
MIFARE Plus 2K, SE(1K) (7 Byte UID)	00 44	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0
MIFARE Plus 4K (7 Byte UID)	00 42	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0

[1] The 7 byte UID MIFARE Classic 1K has bit 7 = 1, even if the 4 byte NUID mapping is enabled.
[2] The 7 byte UID MIFARE Classic 4K has bit 7 = 1, even if the 4 byte NUID mapping is enabled.

Never use ATQA to identify a chip or to extract UID size. Use the GetVersion command, and if not supported, follow the ISO/IEC 14443-3 card activation sequence (Fig 1 and 2 of this document) based on SAK. ATQA can be collided and misleading.

2.3.1 Coding of ATQA for MIFARE Implementation

In case of MIFARE Implementation, ATQA bits shall be set according to ISO14443-3, mentioning the UID size and if anti-collision is supported or not, all other RFU and propriety bits shall be set to 0.

Note: If the MIFARE implementation is going to be used in a running infrastructure where the existing infrastructure makes use of ATQA for PICC identification and or selection (although always recommended NOT to use), then there shall be an option in the implemented device for configuring the ATQA as required for this legacy application.

2.4 Coding of Select Acknowledge (SAK)

Table 6 shows the coding of the SAK of the NXP card ICs as described in the ISO/IEC 14443-3. It indicates the ISO/IEC 18092 protocol compliance, too. The RFU marked bits must be set to “0”, the proprietary bits might be used for proprietary coding.

In case of double size UIDs or triple size UIDs always **only** the last SAK shall be used to distinguish the chip type.

Note: RIDs always use the size of single size.

Table 5. UIDs (4 Bytes) SAK coding of NXP Contactless Card ICs which do not support a GetVersion command

Coding according to the ISO/IEC 14443-3 and ISO/IEC 18092, X = do not care

CL: Cascade Level

Bit number	UID size	Memory	Sec. Level	Hex Value	8	7	6	5	4	3	2	1
UID not complete				04	0	0	0	0	0	1	0	0
UID complete, PICC compliant with ISO/IEC 14443-4					X	X	1	X	X	0	X	X

Table 5. UIDs (4 Bytes) SAK coding of NXP Contactless Card ICs which do not support a GetVersion command*...continued*

Coding according to the ISO/IEC 14443-3 and ISO/IEC 18092, X = do not care

CL: Cascade Level

Bit number	UID size	Memory	Sec. Level	Hex Value	8	7	6	5	4	3	2	1
UID complete, PICC not compliant with ISO/IEC 14443-4					X	X	0	X	X	0	X	X
UID complete, PICC compliant with ISO/IEC 18092 (NFC)					X	1	X	X	X	0	X	X
UID complete, PICC not compliant with ISO/IEC 18092					X	0	X	X	X	0	X	X
MIFARE Ultralight C CL2	double			00	0	0	0	0	0	0	0	0
MIFARE Classic 1K	single	1K	-	08	0	0	0	0	1	0	0	0
MIFARE Classic 4K	single	4K	-	18	0	0	0	1	1	0	0	0
MIFARE Classic 1K CL2	double	1K	-	08	0	0	0	0	1	0	0	0
MIFARE Classic 4K CL2	double	4K	-	18	0	0	0	1	1	0	0	0
MIFARE Plus	single	2K,SE (1K)	1	08	0	0	0	0	1	0	0	0
MIFARE Plus	single	4K	1	18	0	0	0	1	1	0	0	0
MIFARE Plus CL2	double	2K, SE (1K)	1	08	0	0	0	0	1	0	0	0
MIFARE Plus CL2	double	4K	1	18	0	0	0	1	1	0	0	0
MIFARE Plus	single	2K	2	10	0	0	0	1	0	0	0	0
MIFARE Plus	single	4K	2	11	0	0	0	1	0	0	0	1
MIFARE Plus CL2	double	2K	2	10	0	0	0	1	0	0	0	0
MIFARE Plus CL2	double	4K	2	11	0	0	0	1	0	0	0	1
MIFARE Plus	single	2K, SE (1K)	3	20	0	0	1	0	0	0	0	0
MIFARE Plus	single	4K	3	20	0	0	1	0	0	0	0	0
MIFARE Plus CL2	double	2K, SE (1K)	3	20	0	0	1	0	0	0	0	0
MIFARE Plus CL2	double	4K	3	20	0	0	1	0	0	0	0	0

Note: The bit numbering in the ISO/IEC 14443 starts with LSBit = bit 1, but not LSBit = bit 0. So one byte counts bit 1…8 instead of bit 0…7.

Note: NXP MIFARE Plus ICs might use a **generic SAK**, which does not (exclusively) indicate the chip type during the anti-collision procedure for privacy reasons. In such case the way to distinguish between different MIFARE Plus types is the read of Block 0, to use the ATS, if available, or the card capabilities of the Virtual Card Selection.

Note: The MIFARE Classic EV1 1K, MIFARE Classic EV1 4K with 7 byte UID (Double Size UID) with NUID mapping enabled does not support Cascade Level 2, and therefore uses the indicated SAK in Cascade Level 1.

2.4.1 Coding of SAK for MIFARE implementation

In case of MIFARE implementation, final SAK shall be set according to ISO14443-3 and MIFARE SAKs. In case of multi-MIFARE implementation, all supported SAKs can be ORed to generate a SAK to be presented. In case of UICC, sometimes the CLF itself can set some bits showing activated applications. Following table (Table 6) shows some examples.

Table 6. SAK example for multiple MIFARE implementations

Example	Final SAK values					
	MIFARE Classic 1KB SAK = 0x08 (b4 is set)	MIFARE Classic 4KB SAK = 0x18 (b5,b4 are set)	MIFARE DESFire SAK = 0x20 (b6 is set)	P2P support from Android SAK = 0x40 (b7 is to be set)	Standard ISO1443-4 (b6 is set)	Resultant SAK
Example 1	X	-	X	-	-	0x28
Example 2	-	X	X	-	-	0x38
Example 3	-	X	-	-	X	0x38
Example 4	X	-	X	X	X	0x68
Example 5	-	-	-	X	X	0x60
Example 6	-	X	X	X	X	0x78
Example 7	X	-	-	-	X	0x28

Note: SAK is a bit mapping and is recommended to use the bit to check the MIFARE type, the full value of SAK shall not be used to detect a MIFARE type. For detail check in the application note AN10834.

In future, NXP recommends using “Virtual Card Architecture (VCA)” for PICC selection and type identification. If installations do not depend on the actual content of ATQA, SAK and/or ATS(see Section 2.5) for card selection and identification, this allows for more than one MIFARE product being enabled for activation in a single device at the same time. In this case, the VCA allows for efficient and privacy friendly selection of the targeted MIFARE product. This is described in a separate application note [2].

2.5 Coding of Answer To Select (ATS)

As the ATS of different MIFARE ICs can be customized, it is certainly not advisable to rely on the ATS to differentiate the IC type. NXP advises to keep the default value of the ATS to avoid any privacy attack based on the information in ATS.

3 References

1. **AN10834 - MIFARE ISO/IEC 14443 PICC Selection** - available on nxp.com, https://www.nxp.com/docs/en/application-note/AN10834.pdf
2. **AN12057 - Making reader infrastructures ready for multi-application cards and devices** - available on nxp.com, https://www.nxp.com/docs/en/application-note/AN12057.pdf
3. **AN4513 - Reader infrastructure requirements to support risk managed MIFARE 2GO software solution** - available on DocStore

4 Legal information

4.1 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.

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.

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.

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.

4.3 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 Classic — 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.

NTAG — is a trademark of NXP B.V.

SmartMX — is a trademark of NXP B.V.

Tables

Figures

Contents

Date of release: 10 January 2023
Document identifier: AN10833