AN12057

Making reader infrastructures ready for multi-application cards and devices

Rev. 1.1 — 15 June 2021
445611

Application note
COMPANY PUBLIC

Document information

Information	Content
Keywords	Reader terminal, terminal applications, PTO, reader infrastructure, contactless, MIFARE, SmartMX, JCOP, NFC, NFC mobile device, multi-application environment
Abstract	This document gives recommendations on reader and terminal implementations regarding the conformity towards ISO/IEC standards. It focuses on the acceptance of contactless cards and NFC mobile devices hosting multiple applications.

Revision history

Revision history

Rev	Date	Description
1.1	20210615	Links in Section 5 updated
1.0	20171003	Initial version of the document

1 Introduction

1.1 Motivation and background

Today many transport ticketing, access management, loyalty, and much more systems use contactless cards compliant to ISO/IEC 14443 in their infrastructure. Terminals are typically designed to operate a well determined set of cards, holding specific applications. This is also known as closed system approach. Intentionally or not, some terminal applications require specific parameter settings of lower RF or ISO protocols to perform the entire transaction. In case the mentioned parameters are not set accordingly by the card or the NFC mobile devices (NMD) emulating a card, the terminal application may stop the transaction. NMDs may host multiple applications. Typically, those applications may rely on different or even conflicting low level ISO/IEC 14443 parameter settings, which may cause interoperability issues.

In order to avoid interoperability issues with multi-application cards and NMDs, this document aims to list contactless parameters and to provide guidance on its relevance and their settings in a reader infrastructure system. Additionally, possible consequences which can arise in case guidelines are neglected, are mentioned.

1.2 Scope

This application note addresses system operators, system integrators, infrastructure providers and terminal developers which aim to allow multi-application cards and NMDs in their system. Thus, aim to move from a closed to an open ecosystem approach. The document attempts to allow the coexistence of multiple applications, to be used within one reader system.

1.3 Important remark

This application note is a supplementary document, highlighting essential parts of ISO/IEC 14443, ISO/IEC 7816, ISO/IEC 18092 parameters and their usage in reader systems.

In order to get the full picture of the mentioned standards and products, please refer to the matching specifications, whitepapers and datasheets.

1.4 Symbols and abbreviated terms

AID Application Identifier

APDU Application Protocol Data Unit

ATQA Answer to Request

ATR Answer to Reset

ATS Answer to Select

C-APDU Command APDU (sent from the PCD to PICC)

CID Card Identifier

CL Cascade Level

CT Cascade Tag

FSC Frame Size for Proximity Card

FSCI Frame Size for Proximity Card Integer

FSD Frame Size for Proximity Device

FSDI Frame Size for Proximity Device Integer

FWI Frame Waiting Integer

FWT Frame Waiting Time

HCE Host Card Emulation

IC Integrated Circuit

LSB Least Significant Byte

NAD Node Address

NFC Near Field Communication

NMD NFC Mobile Device

PCD Proximity Coupling Device

PICC Proximity Integrated Circuit Card

PPS Protocol and Parameter Selection

R-APDU Response APDU (sent from PICC to PCD)

RATS Request for Answer to Select

REQA Request A

RID Random ID

SAK Select Acknowledge

SE Secure Element

UICC Universal Integrated Circuit Card

UID Unique Identifier

WTX Waiting Time Extension

2 General guidelines for infrastructures / reader systems

2.1 Currently existing issues

Already installed reader infrastructures are mostly not prepared for 3rd party media. ISO/IEC 14443 and ISO/IEC 18092 offer several different ways how to exchange information and provide optional features. It is not required to implement optional features.

In the past, PCD implementations in the field were mainly designed to allow single application PICCs indicating specific parameter settings. As a result, reader of such an infrastructure rejected all other PICCs which made use of different ISO/IEC conformant parameter settings and hosting different applications.

End customers are struggling with the vast amount of different cards in their wallet, all hosting a single application. Therefore, there is a strong trend that PICCs and NMDs are entering the market capable to host multiple applications. Parts of the existing infrastructure do not allow this introduction because of the above mentioned reasons.

It is strongly recommended that the current PCD infrastructure is updated to support the needs of end customers. Especially it shall be achievable to have different kinds of applications (e.g. public transport, access and payment applications) residing on the same device. In order to achieve this, this document gives recommendations how infrastructures can be designed, focusing mainly on ISO/IEC 14443 parameter settings and application selection.

2.2 General recommendations

It is recommended that terminal implementations do not mix up the transport layer (Type A activation and protocol) of the 13.56 MHz radio and the application layer (applicative data). Consequently, terminals should be designed in a way, to accept the whole range of PICC or NMD indicated parameters and to comply with all requirements as specified by ISO/IEC 14443 parts 1 to 4, ISO/IEC 18092 and NFC Forum.

The terminal shall allow the indication, and shall respect all responses coming from the PICC for the following parameters:

- All UIDs and UID lengths (4, 7 and 10 bytes, see [8], section 6.5.4)
- All protocols (see [9], section 11.2.1)
- All bit rates
- All frame sizes and frame waiting times
- All information of the ATS (if within the ISO/IEC 14443 specification)

It is not recommended that the terminal rejects PICCs in case the length of the ATS is not as expected, i.e. does not contain the expected length of historical byes.

3 ISO/IEC 14443 guidelines for terminal implementations

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

For all reader terminals, we recommend to strictly follow the requirements and guidelines of ISO/IEC 14443 and to be non-restrictive regarding the presented parameters by the PICC. In order to work smoothly with different kinds of PICCs / NMDs and their applications, the reading device shall be open and not restrictive on the parameters which are presented by the PICC.

3.1 Implementation of MIFARE ISO/IEC 14443 PICC selection

The ISO/IEC 14443 standard describes how to select and activate a single PICC. By following the recommended card activation procedure, it is guaranteed that a single PICC is properly selected and also keeps on properly selected during the ongoing transaction – independent on the number of cards moved in to the field simultaneously.

Details on the recommended card activation sequence, which includes multiple steps, like the polling for cards, is described in detail in [1].

Especially the timing parameters during card activation and PICC selection are essential. Some important timing constraints, which need to be highlighted:

- After the RF reset was executed, it is necessary to wait at least 5.1 ms before transmitting a REQA or REQB.
- If a terminal polls for multiple technologies, i.e. polls for ISO/IEC 14443 Type-A and Type-B and more, it is necessary to wait at least 5.1 ms between a REQA and a REQB or REQB and REQA. For more details on timing requirements when polling for multiple technologies, please refer to [6].

More detailed information and sequence diagrams which focus on timing constraints, can be found in [1].

3.2 Handling of exchanged ISO/IEC 14443 parameters

During the ISO/IEC 14443 compliant anti-collision loop and card activation, a number of parameters is exchanged between PCD and PICC:

Table 1 lists selected parameters defined in the standards ISO/IEC 14443, ISO/IEC 18092 and NFC Forum. Recommendations on how a PCD should handle each of these parameters are provided. Parameters of particular importance are also discussed in the sections following the table.

For identifying the type of presented PICC, the exchanged parameters need to be evaluated (mainly the content of the SAK). Details for type identification mechanisms can be found in [2].

Table 1. Parameters according to ISO/IEC 14443 and ISO/IEC 18092

Parameter	PCD Recommendation	PICC Recommendation	Comment
RF Field Off	The PCD shall switch off the RF Field for at least 5.1 ms after each cycle of polling or after the deactivation of the PICC.	The PICC shall detect this RF Field Off period to reset all internal states.	
RF Field On	The PCD shall provide an unmodulated RF Field for at least 5.1 ms before sending the first command for activation.	The PICC shall detect this RF Field On period to lock its clock and boot the internal processing within 5 ms.	Some PICCs can respond much faster, but more complex systems need more time to establish an accurate communication.
UID (UID size bit frame in ATQA)	The PCD shall accept any UID that the PICC provides. The PCD shall not rely on a specific length of the UID or on a specific type of the UID. Most important, the PCD shall not rely on a specific range of UIDs for a dedicated application. In case multiple applications are available on the PICC at the same time, it is not predictable, which UID will be presented during the activation (due to the implicit selection).	The PICC may provide any possible type of UID (e.g. random ID or fixed ID) as well as any possible length of UID (4 bytes, 7 bytes or 10 bytes). Most NMDs will provide 4 byte random IDs according to ISO/IEC 18092.	PCD implementations may rely on fixed UIDs or fixed length UIDs (e.g. for executing a key diversification). If this is the case and a device with random ID is presented, the real UID needs to be retrieved by implementing additional commands (e.g. Cmd.GetCardUID for MIFARE DESFire). Random ID may prevent fraudulent tracking and improves card holders privacy protection.
ATQA	The PCD shall not examine or depend upon the values returned by the PICC in b8 to b7 and b5 to b1 of byte 1 and in b4 to b1 of byte 2 of the ATQA.	The PICC shall set the ATQA as defined in ISO/IEC 14443-3.	
SAK (protocol indication)	The PCD shall check for ISO/IEC 14443-3 based applications before evaluating Bit6 and Bit7 of the SAK. The PCD shall accept any value of Bit7. In the mobile environment, this bit mostly is set to 1 to indicate the NFC-DEP capability. The PCD shall not be confused when receiving a Bit7 different to zero, but shall continue normal operation.	The PICC shall have Bit6 set in case any ISO/IEC 14443-4 compliant application is available. The PICC shall have Bit7 set in case any ISO/IEC 18092 compliant application is available (this is the default for NFC mobile devices).	Bit6 and Bit7 indicate the presence of a higher transport protocol. It is possible that applications based on ISO/IEC 14443-3 reside on the PICC independent of the Bit6 or Bit7 setting.
Frame size	The PCD shall indicate its maximum acceptable frame size for receiving data in the FSDI. The PCD shall accept any FSCI value within the valid range received from the PICC.	The PICC shall indicate it`s maximum acceptable frame size for receiving data in the FSCI. The PICC shall allow any FSDI value proposed by the PCD.	Some PCD implementations may be restricted to specific combinations.

Table 1. Parameters according to ISO/IEC 14443 and ISO/IEC 18092*...continued*

Parameter	PCD Recommendation	PICC Recommendation	Comment
Frame waiting time	The PCD shall evaluate the FWI and allow any received value within the valid range. The default FWI is 4. Until the RFU value 15 is assigned by ISO/IEC, a PCD receiving FWI = 15 should interpret it as FWI = 4.	The PICC shall indicate it`s FWI (possible values between 0 to 14). If specific commands require longer processing time, a S(WTX), a frame waiting time extension request, can be sent.	Some PCD implementations may be restricted to specific FWI settings.
SFGI	The PCD shall evaluate the SFGI and allow any received value within the valid range. The default FWI is 0. Until the RFU value 15 is assigned by ISO/IEC, a PCD receiving SFGI = 15 should interpret it as SFGI = 0.	The PICC shall set the SFGI as defined in ISO/IEC 14443-4.	
Bit rates	The PCD shall accept any indicated bit rate as received within the ATS, however does not necessarily need to use the highest bit rate.	The PICC shall indicate the maximum supported bit rate in the Interface byte TA(1) or via S(PARAMETER) negotiation.	
CID supported	The PCD shall accept PICCs supporting CID as well as PICCs not supporting CID. The PCD shall continue normal operation independent if the PICC supports or does not support CID.	The PICC shall indicate whether CID is supported or CID is not supported.	The CID supported flag is located in Bit1 of the Interface Byte TC(1) of the ATS.
NAD supported	The PCD shall allow any possible value for the NAD supported field. Independent whether it receives NAD supported or NAD not supported, it shall be accepted.	The PICC shall indicate whether NAD is supported or NAD is not supported.	The NAD supported flag is located in the Bit2 of the Interface Byte TC(1). NAD is rarely supported by PICCs nowadays.
Historical bytes	The PCD shall allow any possible value for the historical bytes and shall not restrict them to certain expected values.	The PICC is free to use the historical bytes as they are optionally available. The maximum number of historical bytes can be determined from the maximum length of the ATS.	The content of the historical characters is not fixed. They can be used for any specific information of the PICC provider. Accepting only certain defined historical bytes on the PCD might lead to interoperability issues.

3.2.1 Terminal implementations supporting only ISO/IEC 14443-3 applications

In case the PICC indicates the presence of ISO/IEC 14443-4 applications in the SAK, the PCD shall nevertheless send commands for the ISO/IEC 14443-3 based applications.

3.2.2 Terminal implementations supporting both ISO/IEC 14443-3 applications and ISO/IEC 14443-4 applications

Independent if the PICC indicates the presence of higher layer protocols in the SAK, the PCD shall check for the existence of ISO/IEC 14443-3 applications by sending the according commands. In case no ISO/IEC 14443-3 application is found, the PICC may have left the ACTIVE state and entered the IDLE state. In that case the PCD should

perform a card activation and put the PICC in the PROTOCOL state, before the PCD can check for existing ISO/IEC 14443-4 applications.

3.3 Overcoming potential restrictions with respect to the FWI

Especially NMDs may hold several applications, where from each application can be characterized by different RF parameters. Some applications require the PICC to set the FWI to a specific value.

On the PCD side the interoperability should not be affected by this specific setting, as the terminal shall respect any FWI value up to FWI = 14. PCDs which expect a certain FWI value (e.g. 7 or 8) are neither ISO/IEC 14443 nor EMVCo compliant.

4 Additional recommendations

4.1 Host Card Emulation (HCE) and ISO/IEC 7816 support

Especially for the support of HCE implementations, future terminal implementations shall be designed and implemented in a way that application selection according to the underlying (native) PICC command set based on ISO/IEC 14443-4, as well as application selection according to ISO/IEC 7816, can be achieved.

Beside the host, NMDs may contain a Secure Element (SE) such as the SmartMX. In this case, several NFCEEs (NFC execution environments) are available on the NMD. When several NFCEEs are present on one NMD, then the RF parameters which are presented to the terminal can be of any of the available NFCEEs or from the managing entity. Depending on the selected default application of the NMD and its location (either the SE or the host), the UID might change. Consequently, the PCD targeted application may not match the received UID. Therefore, the PCD shall select applications regardless of the received UID.

Example: Using HCE it is possible to activate the card emulation with parameters of SmartMX, but finally an application residing on the host is selected by the terminal application. The SmartMX and the host might have different UIDs, and the application does not know the UID of the SmartMX. The expected behavior in this example is that the terminal does the activation process using the RF parameters that are presented by SmartMX, and on the NMD the NFC controller takes care for routing the request to the application which is residing on the host. For this routing, the NFC controller uses a routing table where all the AIDs of SmartMX and host are mapped.

4.1.1 Application selection using the SELECT FILE command

For application selection according to ISO/IEC 7816-4, the command SELECT FILE by DF Name needs to be used in the terminal implementation (with the DF Name representing the AID of the application), see details in [4], section 3.3.

This application selection can be used for the interaction with HCE as well as PICCs which operate on ISO/IEC 14443-4 and support the ISO/IEC 7816-4 interindustry-compliant command set (at least the SELECT FILE) command.

Infrastructures which are currently not using the SELECT FILE command, have the possibility to select the DF Name / AID according to the NXP IID Allocation scheme [3]. Existing infrastructures which are already using the SELECT FILE command in their terminal implementations, can use the same DF Name for the HCE application implementation.

4.1.2 UID retrieval

Retrieval of the UID is required mainly when using diversified keys inside the PICC, and the key diversification is based on the UID as a base input of the key diversification function. Also when using special configurations, such as for example the random ID, the real UID needs to be retrieved from the PICC.

The UID reported by an NMD in the ISO/IEC 14443-3 ANTICOLLISION process is determined by the NFC Controller. The Android Host Card Emulation is fully independent of the UID and there is no API available which allows to set it. The UID mainly depends on the default Secure Element that is defined in the NFC controller (either UICC or

SmartMX) and on the implicit selection, in case there are multiple applications available on the SmartMX.

It is possible to fix any value of the UID to a static value of 4 bytes, 7 bytes or 10 bytes by using the according NCI parameter (LA_NFCID1), as defined in [7], if the default route for the card activation is the host.

4.1.3 Usage of Random ID

In case a random ID is used for card activation, the actual mechanism to retrieve the UID is dependent on the concrete product of the MIFARE product family.

To give some examples:

- For MIFARE DESFire, the dedicated commands Cmd.GetVersion or Cmd.GetCardUID can be executed. As a response, the real UID of the PICC will be returned.
- For MIFARE Classic, MIFARE Ultralight and MIFARE Plus a read command to block 0 in sector 0 needs to be executed (read from manufacturer block), where the manufacturer details and the UID are stored.

4.2 MIFARE4Mobile

Detailed recommendations regarding how to handle MIFARE4Mobile on the terminal installation is given in [5].

4.2.1 Usage of UIDs in MIFARE4Mobile

Depending on the MIFARE4Mobile usage, and if a Virtual Card is activated by implicit selection (e.g. MIFARE Classic), the UID presented by the cell phone can be:

- Random UID, changing at each new activation
- Fixed 7 bytes UID, corresponding of the Master UID of the secure element (like P73)
- Pseudo Random UID (4-bytes or 7-bytes) using a random ID in a pre-defined range and fixed during the creation of the Virtual Card
- Assigned 4-bytes or 7-bytes UID if application has full access to the Secure Element

4.3 RF field of the reader / terminal

As already stated in a previous section of this document, all timing-related parameters during card activation and PICC selection are essential. For modifications on the RF field (field on / field off), at least 5.1 ms waiting time need to be inserted before continuing with command execution.

5 References

[1] **Application note —** AN10834 MIFARE ISO/IEC 14443 PICC Selection, available on the NXP website at the following link: https://www.nxp.com/docs/en/application-note/AN10834.pdf

[2] **Application note —** AN10833 MIFARE Type Identification Procedure, available on the NXP website at the following link: https://www.nxp.com/docs/en/application-note/AN10833.pdf

[3] **Application note —** AN11909 How to create an Installation Identifier (IID), available on the NXP website at the following link: https://www.nxp.com/docs/en/application-note/AN11909.pdf

[4] **Application note —** AN11704 MIFARE DESFire Application Development Guidelines, document number 3363xx, available in NXP DocStore

[5] **Whitepaper —** GSMA MIFARE4Mobile Implementation Guidelines, GMSA, April 2015, available on the GSMA Website at the following link: http://www.gsma.com/digitalcommerce/wp-content/uploads/2015/04/GSMAM4MIG-15042015.pdf

[6] **Specification —** NFC Activity Specification, Technical Specification, NFC Forum, Version 1.1, 2016-08-08

[7] **Specification —** NFC Controller Interface (NCI) Specification, Technical Specification, NFC Forum, Version, 2.0, 2017-04-19

[8] **Standard —** ISO/IEC 14443-3 International Standard, Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anticollision, Third edition 2016-06-01

[9] **Standard —** ISO/IEC 18092 Information technology – Telecommunications and information exchange between systems – Near field Communication – Interface and Protocol (NFCIP-1)

6 Legal information

6.1 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.

6.2 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 — Customer understands that all NXP products may be subject to unidentified or documented vulnerabilities. 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.

6.3 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.

6.4 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.

Tables

Tab. 1. Parameters according to ISO/IEC 14443 and ISO/IEC 18092 7

Contents

1 Introduction 3
1.1 Motivation and background 3
1.2 Scope 3
1.3 Important remark 3
1.4 Symbols and abbreviated terms 3
2 General guidelines for infrastructures / reader systems 5
2.1 Currently existing issues 5
2.2 General recommendations 5
3 ISO/IEC 14443 guidelines for terminal implementations 6
3.1 Implementation of MIFARE ISO/IEC 14443 PICC selection 6
3.2 Handling of exchanged ISO/IEC 14443 parameters 6
3.2.1 Terminal implementations supporting only ISO/IEC 14443-3 applications 8
3.2.2 Terminal implementations supporting both ISO/IEC 14443-3 applications and ISO/IEC 14443-4 applications 8
3.3 Overcoming potential restrictions with respect to the FWI 9
4 Additional recommendations 10
4.1 Host Card Emulation (HCE) and ISO/IEC 7816 support 10
4.1.1 Application selection using the SELECT FILE command 10
4.1.2 UID retrieval 10
4.1.3 Usage of Random ID 11
4.2 MIFARE4Mobile 11
4.2.1 Usage of UIDs in MIFARE4Mobile 11
4.3 RF field of the reader / terminal 11
5 References 12
6 Legal information 13

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

Date of release: 15 June 2021
Document identifier: AN12057
Document number: 445611