NT4H1321

NTAG 413 DNA Secure Unique NFC Message for direct access to web services

Rev. 3.2 — 12 October 2017
400232

Product short data sheet
COMPANY PUBLIC

1 Introduction

NTAG 413 DNA revolutionizes NTAG product portfolio by bringing AES cryptographic authentication and allows to automatically and securely connect to a web service by just tapping the tag without the need of a dedicated app installed on the mobile NFC device.

Besides the NXP originality signature and a 3-pass mutual authentication, it introduces a novel security feature called “Secure Unique NFC Message (SUN)”, which automatically generates tap-unique tag authentication data upon each read-out what enables dedicated unique communication to each user based on predefined criteria. No app (in NFC device) is required to generate this tap-unique data consisting of CMACed information derived from the chip UID, a tap counter and contained data. An NFC enabled device can automatically connect to a web based service and based on the information contained in URL, the device can check the tags authenticity and verify the information validity. NTAG 413 DNA offers flexibility to individualize the structure of this unique data set.

NTAG 413 DNA is an ideal solution to engage with consumers through dynamic content experiences, fully triggered by them and served in real-time. By that it enables smarter marketing based on ongoing contextual and unique consumer engagement opportunities in a secure way. Applications include but are not limited to consumer engagement, brand protection, access control, one-time vouchers and similar use cases where the proof of uniqueness, originality and physical tag presence are required.

NTAG 413 DNA is certified as NFC Forum Type 4 Tag [Certifcation ID: 58515] [15] and is also compliant to ISO/IEC14443-4 [4], ISO/IEC 7816-4 [7] file structure and APDUs format. Thanks to the high input capacitance (70pF), NTAG 413 DNA tag IC is particularly tailored for applications requiring small footprints, without compromise on performance. Small NFC tags can be more easily embedded into e.g. product labels or electronic devices. The mechanical and electrical specifications of NTAG 413 DNA is tailored to meet the requirements of inlay and tag manufacturer.

1.1 Contactless energy and data transfer

Communication to NTAG 413 DNA can be established only when the IC is connected to an antenna. Any form factor and antenna class type according to ISO/IEC 14443-1 [1] is possible to design with NTAG 413 DNA ICs. Few antenna design examples with guidelines are in NTAG antenna design application note [12] .

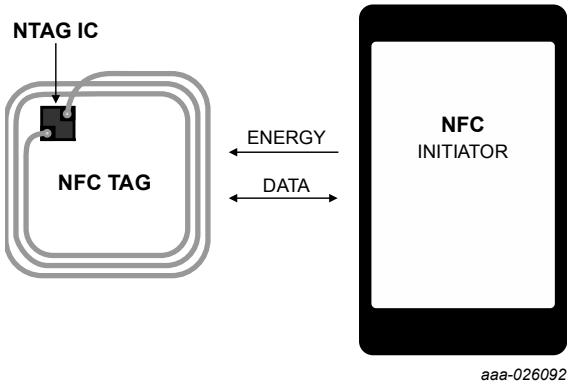

Figure 1. Contactless system

When NTAG 413 DNA is positioned in the RF field, the high speed RF communication interface allows the transmission of the data with a baud rate of up to 424 Kbit/s.

2 Features and benefits

2.1 NTAG 413 DNA features overview

2.1.1 RF Interface & Communication Protocol

- Fully compliant to the ISO/IEC 14443, all parts 1 to 4, [1], [2], [3], [4]
- Fully compliant to the ISO/IEC 7816-4 [7] file selection and APDU handling
- Fully compliant passive target compliant to ISO/IEC18092 [16]
- Features 7-byte UID according to ISO/IEC14443 – 3 [3]
- Communication speed up to 424 kbps

2.1.2 NFC Forum Tag Type compliance

- Fully compliant to the NFC Forum Tag 4 Type technical specification [5]
- Fully compliant to NDEF data structure configurations [6].
- Certified (Certification ID: 58515) NFC Forum Type 4 Tag, which ensures maximum interoperability [6].

2.1.3 Memory organization

- One 32-byte standard data file, formatted as Capability Container (CC)
- One 128-byte standard data file for NDEF message
- Flexible mirroring of UID, NFC Counter and CMAC in the NDEF message
- Configurable separators´ positions, lengths and values (or format) within the NDEF message

2.1.4 Security features

- Secure Unique NFC Message (SUN)
- Three AES 128-bit application keys featuring key versions
- Incremental NFC Counter, which counts each tap

- AES based dynamic CMAC as part of the NDEF data
- Three-pass mutual authentication
- Plain, CMACed and encrypted communication (configurable)
- Secure retrieval of NFC Counter (optional)
- ECC based NXP originality signature
- Tamper-resistant secure hardware

2.1.5 Deployment and user convenience

NTAG 413 DNA offers the personalization of NFC tag with different type of NDEF records and a flexible setting of the NDEF file to define the mirrored parameters and CMAC input offset. At personalization of of the tag, individual application keys, and accessrights to NDEF file with those keys can be set independently.

2.2 Crypto standard

NTAG 413 DNA's core crypto function is compliant to FIPS PUB 197 (FIPS 197) Advanced Encryption Standard (AES) [10]. CMAC is calculated according to NIST Special Publication 800-38B [11], and uses only 8 even bytes from last encrypted block.

2.3 NTAG 413 DNA benefits

2.3.1 Secure Unique NFC Message (SUN)

A cryptographical method which is generating Secure Unique NFC Message (SUN) in each tap based on Secure Dynamic Messaging.

A cryptographical method which is generating Secure Unique NFC Message (SUN) in each tap based on Secure Dynamic Messaging, see the full data sheet [9].

2.3.2 Configuration of the Secure Unique NFC Message

Mirroring items (UID, NFC Counter, CMAC), separators´ positions, lengths and values can be defined for the NDEF data. Upon the first read command within a session, the file content is generated according to the pre-defined settings and will be available thereafter. The data to be included in the CMAC calculation can be configured using an offset.

The NFC Counter is incremented on each tap and the unique response data will be generated along with a CMAC. For connecting directly to a web-service without any dedicated application on an NFC device, the NDEF data to be formatted to a URI record.

2.3.3 Mirroring

2.3.3.1 UID

7-byte fixed UID is programmed in the chip, and can be mirrored within the NDEF message.

2.3.3.2 NFC Counter

A 3-byte up counter is incremented only once per each session when the NDEF file is read. This counter value can be optionally mirrored in plain into the NDEF message. Counter value can be read out encrypted after authentication by using the assigned application key as well.

2.3.3.3 CMAC

The 8-byte CMAC can be optionally mirrored into the NDEF message. CMAC is calculated on the defined message length. It is possible to consider only the UID and/or the NFC Counter for CMAC calculation.

2.3.4 Mutual authentication

NTAG 413 DNA offers 3-pass mutual authentication based on challenge response protocol with the application key. This mutual authentication enables the authentication of the tag and host (who knows the keys) simultaneously.

2.3.5 ECC signature

NTAG 413 DNA offers a static ECC signature calculated on the UID of the chip. This ECC signature can be used to verify the tag's genuineness using the public key provided by NXP [8].

2.3.6 Ultimate product authentication

NTAG 413 DNA features can be integrated to design a robust product authentication. Concatenating of the multiple features e.g. ECC signature, history based UID tracking, SUN and 3-pass mutual authentication to design enhanced reliability in product authentication.

2.3.7 Customization from fab

NXP offers commercially the customization of the chip content (securely key injection known as trust provisioning, personalization of NDEF message and file settings). Refer to [13] for detail.

3 Applications

NTAG 413 DNA has been designed to fit in many NFC tagging applications, particularly where security is required. Several applications (but not limited) are mentioned below:

- Web-based product authentication without any application installed in NFC reader device
- In general product authentication with application installed in NFC reader device
- Access management (logical & Physical)
- Electronic voucher
- Gaming
- Consumer interaction
- Advertisement

- Campaign
- Dynamic credential for web log-in
- Document authenticity

4 Quick reference data

Table 1. Quick reference data
[1] [2]

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
C_i	input capacitance		[3] [4]	66.5	70	73.5	pF
f_i	input frequency			-	13.56	-	MHz
EEPROM characteristics							
t_{ret}	retention time	T_{amb} = 22 °C		50	-	-	year
N_{endu}(W)	write endurance	T_{amb} = 22 °C		200000	500 000	-	cycle
t_{cy}(W)	write cycle time	T_{amb} = 22 °C		-	1	-	ms

[1] Stresses above one or more of the values may cause permanent damage to the device.
[2] Exposure to limiting values for extended periods may affect device reliability.
[3] Measured with LCR meter.
[4] T_{amb} = 22 °C; f_i = 13.56 MHz; 2 V RMS

5 Ordering information

Table 2. Ordering information

Part number	Package		
	Name	Description	Version
NT4H1321G0DUF/xxyy	FFC Bump	8 inch wafer, 75 um thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 160 bytes user memory, 70pF input capacitance	-
NT4H1321G0DUD/xxyy	FFC Bump	8 inch wafer, 120 um thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 160 bytes user memory, 70pF input capacitance	-

xx = fabkey, yy = version

6 Block diagram

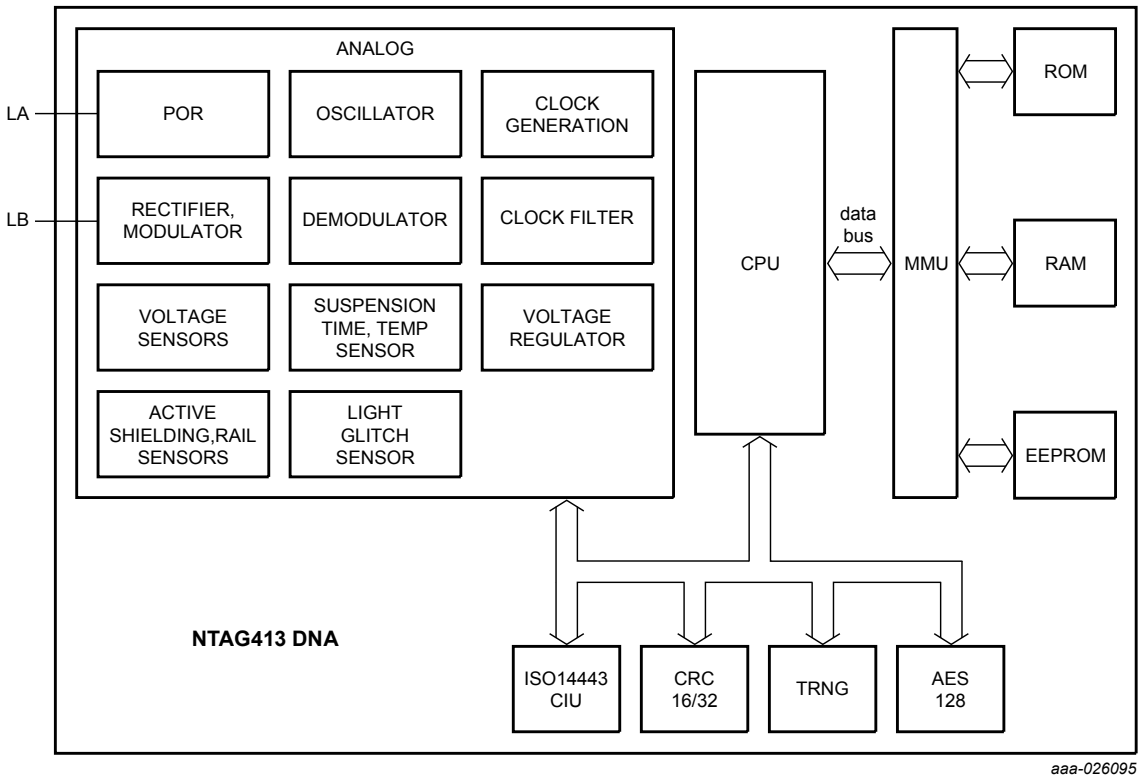

Figure 2. NTAG 413 DNA block diagram

7 Limiting values

Table 3. Limiting values
[1] [2]

Symbol	Parameter	Conditions		Min	Max	Unit
I_i	input current			50	-	mA
$P_{tot/pack}$	total power dissipation per package			200	-	mW
T_{stg}	storage temperature			-55	125	°C
T_{amb}	ambient temperature			-25	70	°C
V_{ESD}	electrostatic discharge voltage		[3]	-	2	kV

[1] Stresses above one or more of the values may cause permanent damage to the device.
[2] Exposure to limiting values for extended periods may affect device reliability.
[3] MIL Standard 883-C method 3015; human body model: C = 100 pF, R = 1.5 kΩ.

8 Functional description

8.1 File system

The file system is according to NFC Forum-TS-Type-4-Tag_2.0 NFC [5]. The application structure, see Figure 3 of NTAG 413 DNA is fixed and optimized to fulfil the requirements of the generic and secure NFC applications. In the single application, there is a set of keys and different access link to those keys can be provided by file settings. Note in the file setting "CC" stands for change configuration whearas the 32-byte file is called CC (Capability Container) file

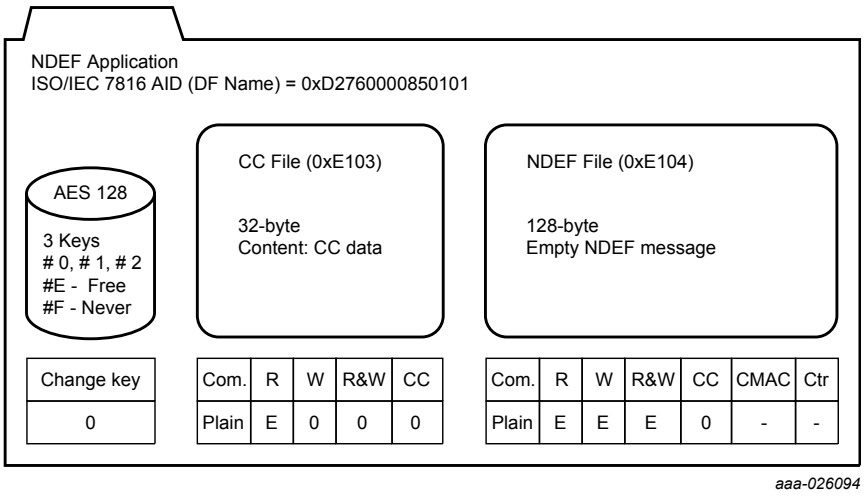

Figure 3. NDEF Application with default setting

8.1.1 Keys

There are three AES 128-bit keys (key number 0, 1, 2) together with key number "E" (means free) and key number "F" (means never). By default these 3-keys can be changed after authentication with key number 0.

8.1.2 CC file

The capability container (CC) file is initialized with the following data field: "000F20010000FF0406E10400800000000000000000000000000000000000000000" present in "INITIALIZED" state. Date structure of the CC file is explained in [5]. It can be updated by authenticating with key number 0. The default access right is set as in Figure 3, write (w), Read &Write (R&W) and change key can be set to any other value or "F" to make this file read only. To be NDEF complaint the read (R) access shall remain free (E). One-byte CC file ID is 0x01, is to be used as file number/ ID for the commands with class byte 0x90, if required.

8.1.3 NDEF file

The NDEF file has an empty NDEF message at delivery. Any NDEF message according to [5] can be written freely in this file. The write access can be changed to any key or to never by authentication with the key number 0. For the NDEF file, the CMAC key and Ctr

read key need to be defined at NDEF personalization. At delivery no keys are defined there and hence the mirroring of UID, NFCCtr, or CMAC are not activated. One-byte NDEF file ID is 0x02, is to be used as file number/ ID for the commands with class byte 0x90, wherever required

8.2 Communication protocol

NTAG 413 DNA uses ISO/IEC7816-4 [7] type standard APDUs for command-response pair.

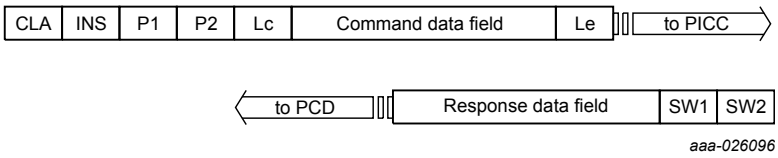

Figure 4. NTAG 413 DNA command response pair

Table 4. Command response pair

Field	Description	Length
Command header	Class byte (CLA)	1
	Instruction (INS)	1
	Parameters (P1,P2)	2
Lc field	Length of command data field (Lc), absent if no data field.	1
Command data field	Absent if no data	Lc
Le field	Expected response length.	1
Response data field	Response data if any, absent if no response data	up to Le
Response trailer	status byte (SW1SW2)	2

The field length and presence might vary for different commands, refer to the specific command description.

8.3 Communication modes

NTAG 413 DNA uses plain communication according to NFC Type 4 Tag operation. But it also allows encrypted and CMACed communication (especially for write) in case it is required to update the NDEF (re) personalization in field.

NTAG 413 DNA supports three communication modes. As shown in the following Table 5, the different communication modes are represented by two bits. This representation is used at several places in the document.

Table 5. Supported communication modes

Communication mode	Bit representation	Explanation
`CommMode.Plain`	X0	No protection: message is transmitted in clear
`CommMode.MAC`	01	MAC protection for integrity and authenticity

Communication mode	Bit representation	Explanation
CommMode.Full	11	Full protection for integrity, authenticity and confidentiality

The communication mode defines the level of security for the communication between PCD and PICC.

At application and PICC level, the communication mode is defined by the command itself, as specified in the following table 7. The specified communication mode is applied if there is an active authentication regardless of whether this authentication is required by the command or not.

At file level, the communication mode is defined by the file. The specified communication mode is applied if there is an active authentication. Note however that, under an active authentication, if the only valid access condition for a certain access right is free access (0xE), CommMode.Plain is to be applied. The commands for authentication and changing keys have their own secure messaging rules, as indicated by N/A (not applicable) in Table 6. If there is no active authentication, the command and response are sent in plain (or the command is rejected in the case an authentication is required).

Table 6. Overview of expected command Communication Mode for secure messaging

Command	Communication mode
Cmd.AuthenticateFirst	N/A (command specific)
Cmd.AuthenticateNonFirst	N/A (command specific)
Cmd.ChangeFileSetting	CommMode.Full
Cmd.ChangeKey	N/A (command specific)
Cmd.ReadNFCCounter	CommMode.Full
Cmd.GetFileSetting	CommMode.MAC
Cmd.GetKeyVersion	CommMode.MAC
Cmd.GetVersion	CommMode.MAC
Cmd.ReadData	CommMode of targeted file.
Cmd.SetConfiguration	CommMode.Full
Cmd.WriteData	CommMode of targeted file.

9 Supported commands and APDUs

Table 7. NTAG413 DNA APDUs

Command	C-APDU (hex)							R-APDU	
INS	CLA	INS	P1	P2	Lc	Data	Le	Data	SW1 SW2
Cmd.SELECT	00	A4	XX	XX	XX	Data to send	XX	response	9000
Cmd.READ BINARY	00	B0	XX	XX	-	-	XX	response	9000
Cmd.UPDATE BINARY	00	D6	XX	XX	XX	Data to write	-	-	9000
Cmd.AuthenticateFirst	90	71	00	00	XX	Reference data	00	Data	9100
Cmd.AuthenticateNonFirst	90	77	00	00	XX	Data	00	Data	9100
Cmd.ChangeFileSetting	90	5F	00	00	XX	Data	00	Data	9100

Command	C-APDU (hex)							R-APDU	
Cmd.GetFileSetting	90	F5	00	00	01	File number	00	Data	9100
Cmd.ChangeKey	90	C4	00	00	xx	data	00	data	9100
Cmd.GetKeyVersion	90	64	00	00	01	Key number	00	Data	9100
Cmd.GetVersion	90	60	00	00	-	-	00	Data	9100
Cmd.ReadNFCCounter	90	F6	00	00	01	02	00	Counter	9100
Cmd.ReadData	90	AD	00	00	XX	Reference	00	Data	9100
Cmd.WriteData	90	8D	00	00	XX	Data	00	Data	9100
Cmd.SetConfiguration	90	5C	00	00	01	File number	00	Data	9100
Cmd.Read_Sig	90	3C	00	00	01	Signature	00	Data	9190

For details of the APDUs and the values see the full data sheet [9].

10 Abbreviations

Table 8. Abbreviations

Acronym	Description
AES	Advanced Encryption Standard
AID	Application IDentifier
APDU	Application Protocol Data Unit
C-APDU	Command APDU
CC	Capability Container
CLA	Class
CMAC	Cipher-based Message Authentication Code
CRC	Cyclic Redundancy Check
Ctr	Counter
DF	Dedicated File
ECC	Elliptic Curve Cryptography
INS	Instructions
MAC	Message Authentication Code
NFC	Near Field Communication
NDEF	NFC Data Exchange Format
POS	Point Of Service
PICC	Proximity IC Card
R-APDU	Response APDU
RID	Registered ID
SDM	Secure Dynamic Messaging
SSM	Standard Secure Messaging
SUN	Secure Unique NFC Message
UID	Unique Identifier

11 References

[1] ISO/IEC 14443-1:2016, Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1: Physical characteristics

[2] ISO/IEC 14443-2:2016, Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 2: Radio frequency power and signal interface

[3] ISO/IEC 14443-3:2016, Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anti-collision

[4] ISO/IEC 14443-4:2016, Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 4: Transmission protocol

[5] NFC Forum Type 4 Tag Operation Specification 2.0, Technical Specification, T4TOP 2.0, NFCForum-TS-Type-4-Tag_2.0, 2011

[6] NFC Data Exchange Format (NDEF), Technical Specification — NFC Forum, 24.07.2006, Version 1.0

[7] ISO JTC 1/SC 27 Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange. ISO/IEC 7816-4:2005, January 2005.

[8] Application note - NTAG 413 DNA Feature and Hints, doc number 4103xx. available from NXP doc store.

[9] NTAG 413 DNA full data sheet, document number 400310, available from NXP doc store.

[10] National Institute of Standards and Technology (NIST), Specification for the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197, November 2001.

[11] NIST Special Publication 800-38B - Recommendation for Block, Cipher Modes of Operation: The CMAC Mode for Authentication. http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf.

[12] NTAG antenna design application note. http://www.nxp.com/products/identification-and-security/nfc-and-reader-ics/connected-tag-solutions/ntag-ic-plus-explorer-kit-demo-kit:OM5569-NT322E?fpsp=1&tab=Documentation_Tab#nogo

[13] Application note - NTAG 413 DNA Personalization at fab, doc number 4124xx. available from NXP doc store

[14] NIST Special Publication 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf.

[15] NFC Forum Type 4 Tag Operation Specification 2.0, Technical Specification, T4TOP 2.0, NFCForum-TS-Type-4-Tag_2.0, 2011

[16] ISO/IEC 18092:2013 - Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1)

12 Revision history

Table 9. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
NT4H1321_SDS v. 3.2	20171012	Product short data sheet	-	NT4H1321_SDS v. 3.1
Modifications:	• NFC Forum certification added			

Document ID	Release date	Data sheet status	Change notice	Supersedes
NT4H1321_SDS v. 3.1	20170601	Product short data sheet	-	NT4H1321_SDS v. 3.0
Modifications:	• Section 2.1.1 "Communication speed up to 424 kbps" added • Table 1: retention time changed into 50 years			
NT4H1321_SDS v. 3.0	20170508	Product short data sheet	-	NT4H1321_SDS v. 1.0
Modifications:	• Data sheet status changed into "Product short data sheet"			
NT4H1321_SDS v. 1.0	20170329	Objective short data sheet	-	-

[1] Stresses above one or more of the values may cause permanent damage to the device.
[2] Exposure to limiting values for extended periods may affect device reliability.

13 Legal information

13.1 Data sheet status

Document status[1][2]	Product status[3]	Definition
Objective [short] data sheet	Development	This document contains data from the objective specification for product development.
Preliminary [short] data sheet	Qualification	This document contains data from the preliminary specification.
Product [short] data sheet	Production	This document contains the product specification.

[1] Please consult the most recently issued document before initiating or completing a design.
[2] The term 'short data sheet' is explained in section "Definitions".
[3] The product status of device(s) described in this document may have changed since this document was published and may differ in case of multiple devices. The latest product status information is available on the Internet at URL http://www.nxp.com.

13.2 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.

Short data sheet — A short data sheet is an extract from a full data sheet with the same product type number(s) and title. A short data sheet is intended for quick reference only and should not be relied upon to contain detailed and full information. For detailed and full information see the relevant full data sheet, which is available on request via the local NXP Semiconductors sales office. In case of any inconsistency or conflict with the short data sheet, the full data sheet shall prevail.

Product specification — The information and data provided in a Product data sheet shall define the specification of the product as agreed between NXP Semiconductors and its customer, unless NXP Semiconductors and customer have explicitly agreed otherwise in writing. In no event however, shall an agreement be valid in which the NXP Semiconductors product is deemed to offer functions and qualities beyond those described in the Product data sheet.

13.3 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.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

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.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

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.

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.

13.4 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.

13.5 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.

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 October 2017
Document identifier: NT4H1321_SDS
Document number: 400232

Общество с ограниченной ответственностью «МосЧип» ИНН 7719860671 / КПП 771901001
Адрес: 105318, г.Москва, ул.Щербаковская д.3, офис 1107

Данный компонент на территории Российской Федерации

Вы можете приобрести в компании MosChip.

Для оперативного оформления запроса Вам необходимо перейти по данной ссылке:

http://moschip.ru/get-element

Вы можете разместить у нас заказ для любого Вашего проекта, будь то серийное производство или разработка единичного прибора.

В нашем ассортименте представлены ведущие мировые производители активных и пассивных электронных компонентов.

Нашей специализацией является поставка электронной компонентной базы двойного назначения, продукции таких производителей как XILINX, Intel (ex.ALTERA), Vicor, Microchip, Texas Instruments, Analog Devices, Mini-Circuits, Amphenol, Glenair.

Сотрудничество с глобальными дистрибьюторами электронных компонентов, предоставляет возможность заказывать и получать с международных складов практически любой перечень компонентов в оптимальные для Вас сроки.

На всех этапах разработки и производства наши партнеры могут получить квалифицированную поддержку опытных инженеров.

Система менеджмента качества компании отвечает требованиям в соответствии с ГОСТ Р ИСО 9001, ГОСТ РВ 0015-002 и ЭС РД 009

Офис по работе с юридическими лицами:

105318, г.Москва, ул.Щербаковская д.3, офис 1107, 1118, ДЦ «Щербаковский»

Телефон: +7 495 668-12-70 (многоканальный)

Факс: +7 495 668-12-70 (доб.304)

E-mail: info@moschip.ru

Skype отдела продаж:
moschip.ru
moschip.ru_4
moschip.ru_6
moschip.ru_9