AN12366

NTAG 5 - Memory configuration and scalable security

Rev. 1.0 — 9 January 2020 Application note
530510 COMPANY PUBLIC

Document information

Information	Content
Keywords	Configuration and security, NTAG 5 switch, link and boost, plain password, AES mutual authentication
Abstract	Guidelines for configuring NTAG 5 memory and how to set security levels.

Revision history

Rev	Date	Description
v.1.0	20200109	First official released version

1 Abbreviations

Table 1. Abbreviations

Acronym	Description
I^2C	Inter-IC communication
IC	Integrated Circuit
NFC	Near Field Communication
PACK	Password acknowledge
PWD	Password
VCD	Vicinity Coupling Device
VICC	Vicinity Integrated Circuit Card

2 Introduction

This document describes recommended use of the NTAG 5 data protection features. NTAG 5 provides features to enhance security and privacy. To benefit from these commands a customer needs to make changes in the system, programming of the IC and operation on the read points. A safe password and/or key handling procedures are necessary to ensure the integrity of an installation and intended security improvements.

2.1 Potential applications

Protect your device and your data:

- Use your own originality check
- Use an NDEF message in the read-only protected open area
- Use plain password or mutual AES authentication to protect your personal settings
- Split the memory into three independently protected areas

3 Security features

There are two (2) security schemes on NTAG 5 family:

1. Plain Password authentication mode (like on ICODE SLIX2)
2. AES authentication mode as per ISO/IEC 29167-10 Crypto suite AES-128 security services for air interface communications (like on ICODE DNA)

Table 2. NTAG 5 different security on types

NTAG 5 name	Security mode	Type
NTAG 5 switch	Password	NTP5210
NTAG 5 link	Password	NTP5312
NTAG 5 link	Password or AES crypto suite	NTP5332
NTAG 5 boost	Password or AES crypto suite	NTA5332

3.1 Authenticity

3.1.1 Password authentication

Password authentication (32-bit or 64-bit passwords) can be done if communication host (RF or I^2C) provides PWD to the NTAG 5 and if PWD is correct, the NTAG 5 responds with PACK (configurable).

3.1.2 AES-128 authentication

AES-128 authentication provides an option, that an Interrogator (VCD) can check whether counter part (VICC) is authentic - sharing the same secret or key. After successful authentication, RF communication is in plain (not encrypted). If higher degree of security is needed, it can be efficiently done on the whole system level. Also, it can be achieved by using SRAM (volatile) of NTAG 5 as a transport layer and security means are put to the application/system layer in combination with a secure µC.

3.2 Locking byte values

To permanently set certain User memory parts to read-only, locking mechanism is present on NTAG 5. Configurable from both interfaces, from RF it is one way programmable only. In additions, sections of Configuration memory can be locked. After the configuration done, it is recommended to write the appropriate lock conditions and lock the device configuration bytes.

LOCK_BLOCK_ COMMAND_SUPPORTED needs to be set to 1b in CONFIG_2 byte in order to enable LOCK_BLOCK command.

Each bit of NFC Lock Block Configuration lock, locks one memory block. SECTION_LOCK "freezes" NFC Lock Block Configuration.

See example [Section 7.5].

3.3 Protecting access to features

Table 3. NTAG 5 Security features

Feature	NTAG 5 switch	NTAG 5 link	NTAG 5 link	NTAG 5 boost
Type	**NTP52101**	**NTP5312**	**NTP5332**	**NTA5332**
Lock block	yes	yes	yes	yes
Password protect EAS	yes	yes	yes	yes
Password protect AFI	yes	yes	yes	yes
Password protection of read/ write EEPROM	yes	yes	yes	yes
Password protection of PRIVACY	yes	yes	yes	yes
Password protection of DESTROY	yes	yes	yes	yes
Tag authentication	-	-	yes (1)	yes (1)
Mutual authentication	-	-	yes (1)	yes (1)
Negative authentication counter	yes	yes	yes	yes
SRAM protection	-	yes	yes	yes
Configuration Area protection	yes	yes	yes	yes
Session Registers protection	yes	yes	yes	yes

(1) Available after PWD to AES mode switch.

3.4 Different memory areas protection

User EEPORM may be split into three areas. Highest prio has the 16-bit PP_AREA_1 pointer. It defines the start of the AREA_1 and it is the same block address from NFC and I^2C perspective.

Only if the 8-bit NFC_PP_AREA_0-H block address is lower compared to the PP_AREA_1, the lower part is split into NFC AREA_0-L and NFC AREA_0-H. Maximum divisions can be 1 kB as the pointer address is 8 bit.

The page AREA_0-L and AREA_0-H can be defined independently from RF and I^2C perspective. Also access restrictions can be different between RF and I^2C. To split the user EEPROM from I^2C perspective the 8 - bit I2C_PP need to be set accordingly.

The concept is illustrated below.

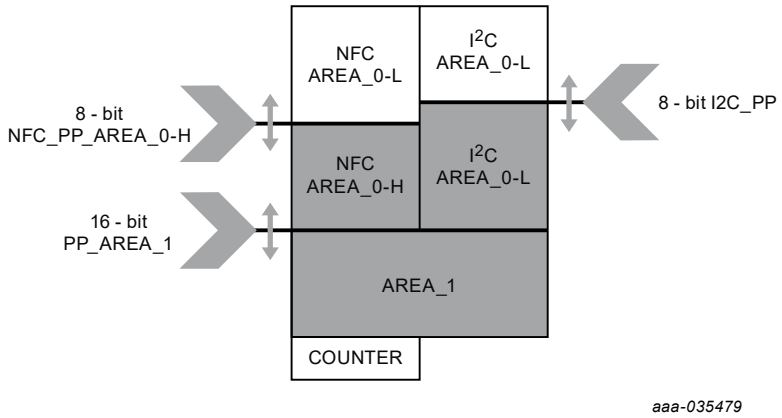


Figure 1. Concept of memory areas

Table 4. NTAG 5 Different memory areas protection possibilities

Memory area	NFC/RF	I^2C
EEPROM	yes (NFC_PP_AREA_0-H)	yes (I2C_PP)
EEPROM - Restricted area	yes (PP_AREA_1)	
SRAM	yes (PWD or Authentication access protection)	no
User Config	yes (PWD or AES)	yes (PWD)
Registers	yes (some)	no

3.5 Reprogrammable originality signature

NXP offers to either lock the pre-programmed NXP originality signature, or to allow customers to re-programm and lock the originality signature.

Following steps for Originality Signature generating and reprogramming are recommended:

1. Generate a public and private key for the parameters secp128r1
2. Create and Sign Originality Signature with private key
3. Verify the Originality Signature with public key
4. Program the Originality Signature into IC memory
5. Lock the Originality Signature

More details with minor adoption change needed can be found in [Application note].

More details on verifying Originality Signature can be found in [Application note].

4 NFC (RF) perspective security

4.1 Plain password

Authentication is done by sharing password in plain over air interface. After successful authentication, respective access rights are granted.

It is a possibility to switch from default 32-bit PWD length to 64-bit PWD length.

4.2 AES mode

Authentication mode as defined in ISO/IEC 15693-3 Amendment 4 and ISO/IEC 29167-10 [International standard]. AES-128 crypto algorithm in CBC mode is used. Interrogator is allowed to perform two (2) auth. procedures:

- Tag authentication (TAM)
- Mutual authentication (MAM)

Switch from PWD to AES mode is available only on NTAG 5 link (NTP5332) and NTAG 5 boost (NTA5332) by setting DEV_SEC_CONFIG byte on block address 3Fh (RF) or 103Fh (I^2C).

In Authentication procedure keys are used only for encryption/decryption and are never exchanged on air interface.

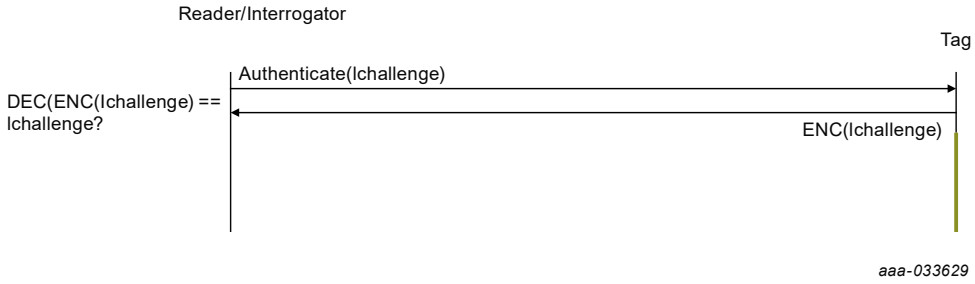
For numerical examples refer to [Application note].

4.2.1 Tag Authentication

Is used to prove the originality of the tapped NTAG 5 (end application, product etc.) with cryptographic authentication. After successful Tag Authentication, the VCD (Interrogator) has a proof that a counterpart VICC (NTAG 5) is authentic - shares the same key.

4.2.1.1 Single NTAG 5 expected in the field

For numerical example follow [Application note].



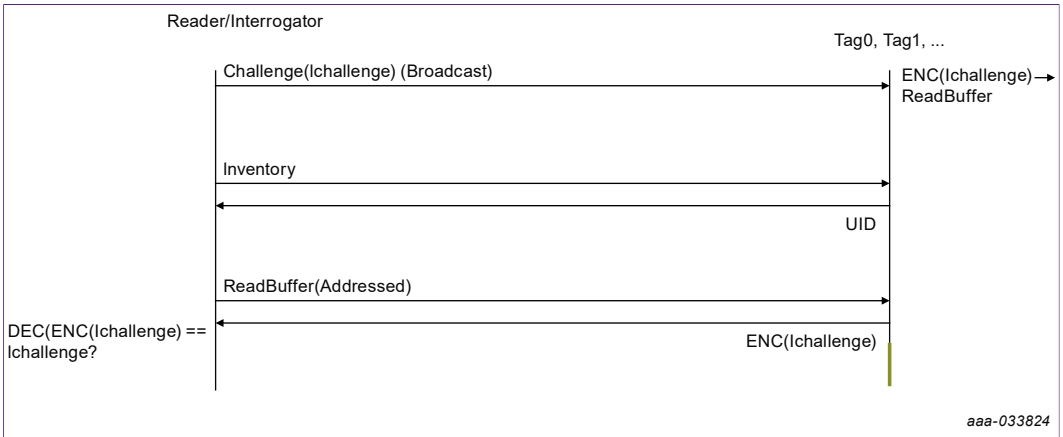
green line = NTAG 5 is Authentic

Figure 2. Single tag Authentication flow

4.2.1.2 Multiple Tags expected in the field

VCD (Interrogator) sends IChallenge command to NTAG 5 or NTAG 5s. After receiving a valid CHALLENGE command the NTAG 5 starts with the crypto calculation and stores the data into it's buffer. If the calculation is finalized, the NTAG 5 will respond to a valid READBUFFER command with the result of the crypto calculation.

VCD (Interrogator) decides which NTAG 5 to address (INVENTORY) before reading the particular NTAG 5's buffer (READBUFFER).

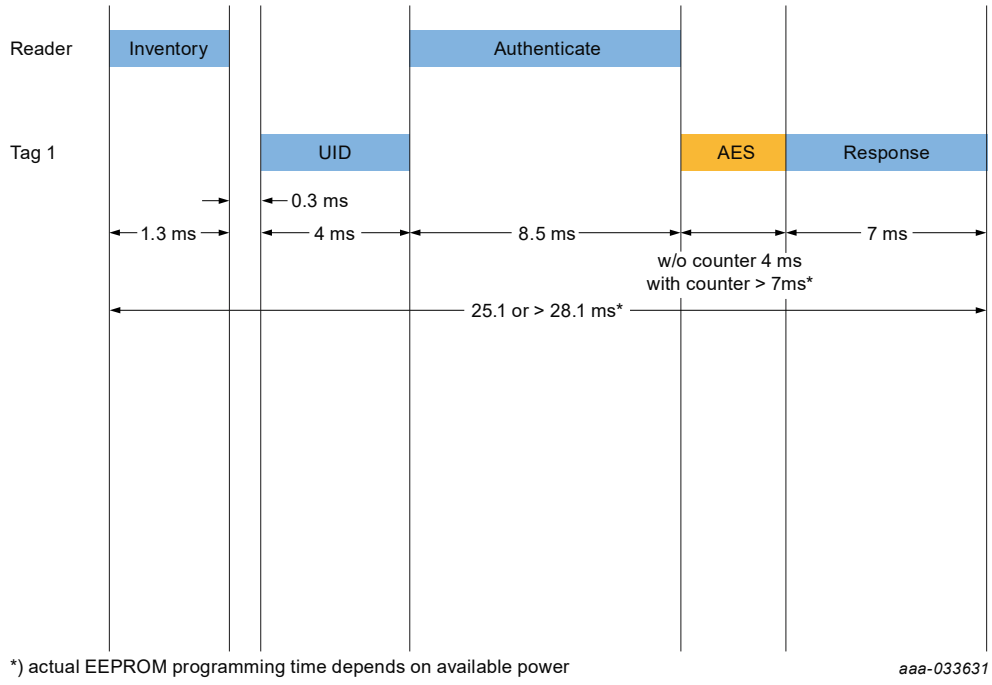


green line = NTAG 5 is Authentic

Figure 3. Tag authentication with multiple NTAG 5 expected in the field

4.2.1.3 Timing measurements

4.2.1.3.1 Single Tag Authentication



counter = Negative Authentication Counter

Figure 4. Single Tag Authentication timings

4.2.1.3.2 Multiple tags - Tag Authentication

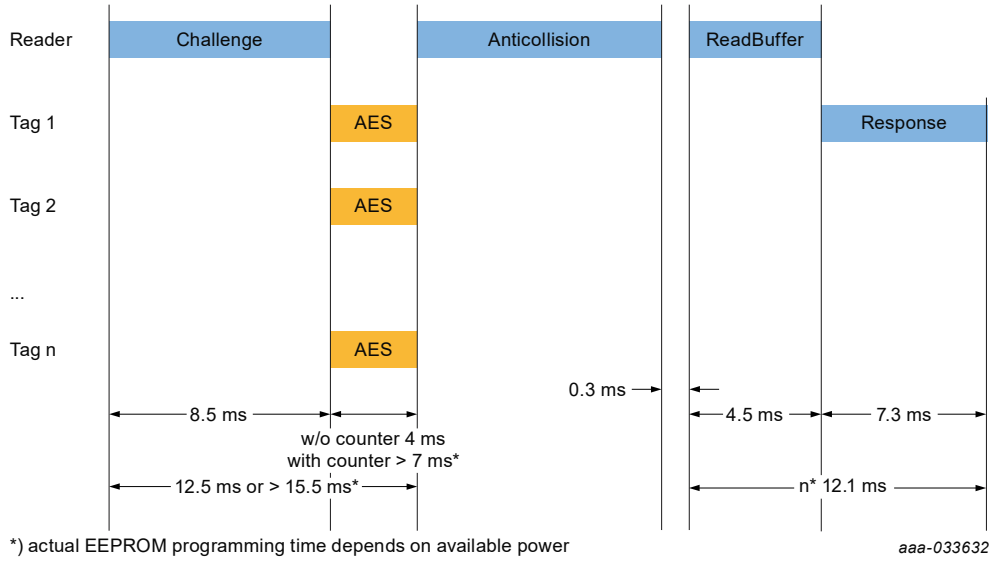


Figure 5. Multiple NTAG 5s - Tag Authentication timings

4.2.2 Mutual Authentication

Is used to protect against unauthorized data access or unauthorized manipulation.

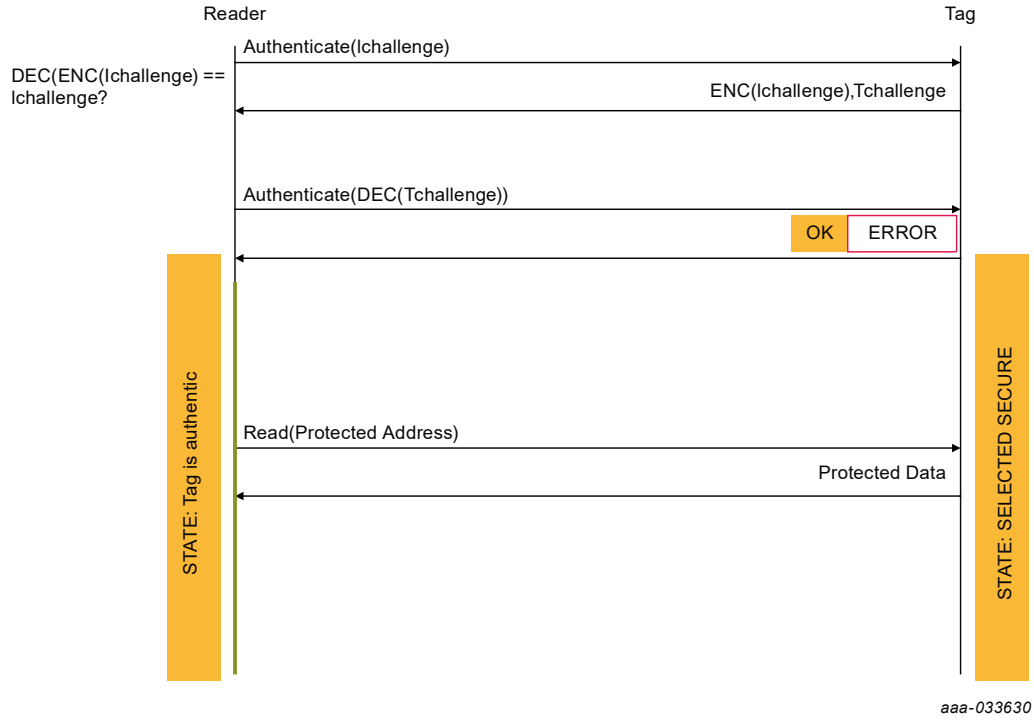


Figure 6. Mutual authentication flow

5 I²C perspective security

I²C Slave communication may be protected by plain password authentication. I²C Host needs to authenticate prior accessing I²C protected areas by writing related password to the related block (blocks 1096h to 1099h).

6 Passwords or Keys generation

The NTAG 5 uses either 32-bit, 64-bit passwords, 128-bit AES keys. This offers a reasonable level of security.

There are several ways to generate a password:

1. Customer generates one set of secret passwords/keys used in all NTAG 5 (e.g. batch)
2. Customer generates different passwords/keys for each NTAG 5 and stores them in a database.
3. Customer uses the UID of the IC and a secure algorithm (free of choice) to calculate diversified passwords/keys for all ICs. (recommended) [Application note]

7 Example: Security protection for the field

In following example memory will be organized as on the figure below.

- UID: E00401581A003F00
- NDEF - URI record:

Block [hex]	Byte0	Byte1	Byte2	Byte3	Area
0000	E1	10	80	00	AREA_0_L
0001	03	13	D1	01	
0002	0F	55	04	6E	
0003	74	61	67	35	
0004	2E	6E	78	70	
0005	2E	63	6F	6D	
0006	2F	FE	00	00	
0007	00	00	00	00	AREA_0_H
0008	11	22	33	44	
0009	55	66	77	88	
...	...	...	...	...	
005F	99	AA	BB	CC	
0060	00	00	00	00	AREA_1
0061	55	55	55	55	
0062	44	44	44	44	
01FE	33	33	33	33	
01FF	counter				

7.1 Write/Store (derived) PWD

- New WRITE PWD value: "11223344h"
- WRITE PASSWORD (password identifier 02h) command code: B4h (Note: PWD values can be written also using direct WRITE CONFIG)
- Put NTAG into SELECTED state or use Addressed mode (UID provided in command payload)

Procedure:

1. GET RANDOM NUMBER
   VCD → VICC: 12 B2 04 (1B B9)
   VICC → VCD: C2 73 + CRC
2. VCD calculates XOR_Password[31:0] = Password[31:0] XOR {Random_Number[15:0], Random_Number[15:0]}. Note: default PWD is 00000000h.
   C2 73 C2 73
3. SET PASSWORD (Authenticate with default PWD)
   VCD → VICC: 12 B3 04 02 C2 73 C2 73 (6C F8)
   VICC → VCD: 00

4. WRITE PASSWORD (Write new PWD)
   VCD → VICC: 12 B4 04 02 11 22 33 44 (12 1B)
   VICC → VCD: 00

7.2 Set Protection Pointer and Pointer Conditions

Write protection pointer configuration:

- NFC_PP_AREA_0-H to value (07h)
- AREA_0_L is:
  - not read protected
  - not write protected
- AREA_0_H is:
  - not read protected
  - write protected

VCD → VICC: 02C1045807200000 (RF-PP, RF-PPC)

7.3 Device Security configuration

The level of security can be defied with the device security configuration (DEV_SEC_CONFIG) and can be written by both interfaces. If locked by security lock cannot be updated anymore by any of the interfaces. The IC RF security features can be chosen between AES tag/mutual authentication or plain password for NTAG 5 boost (NTA5332) and NTAG 5 link (NTP5332) only. NTAG 5 switch (NTP5210) and NTAG 5 link (NTP5312) only offer plain password.

Form RF perspective there are three levels of security:

- 32-bit plain password
- 64-bit plain password
- AES: Available on NTAG 5 boost (NTA5332) and NTAG 5 link (NTP5332)

Security modes can be configured in DEV_SEC_CONFIG (3Fh).

For I^2C perspective only plain password protection is implemented.

7.4 RESTRICTED area configuration

Restricted area protection pointer (PP_AREA_1) set to 60h. Restricted area is always protected from both the interfaces. Area can be defined by 16-bit address. As restricted area has highest priority and overlaps with any of the page L (AREA_0-L) or page H (AREA_0-H), this user area is considered as Restricted area.

VCD → VICC: 02C1043FA500**60**00

After this command, the restricted area is automatically read and write protected by the NFC_PWD5 (AREA_1 Read Password) and NFC_PWD6 (AREA_1 Write Password).

NOTE: When using AES security scheme, the key(s) for the restricted area is/are defined with the related NFC KeyPrevilegies (NFC_KPx).

7.5 Lock memory area (read-only state)

NDEF area (block 0000h - 0006h) set to read-only. It can be done either:

- LOCK BLOCK command (also NFC Forum defined)
- directly writing to Configuration bytes (faster)

Therefore first 7 bits of NFC_LOCK_BL0 needs to be set.

Table 5. Bit set

	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	byte value in [hex]
NFC_ LOCK_ BL0	0	1	1	1	1	1	1	1	7F

Procedure:

1. WRITE CONFIG cmd
   VCD → VICC: 12 C1 04 6A 7F 00 00 00 (A1 18)
   VICC → VCD: 00 + CRC

8 References

[1] NTP5210 - NTAG 5 switch, NFC Forum-compliant PWM and GPIO bridge, doc.no. 5477xx
https://www.nxp.com/docs/en/data-sheet/NTP5210.pdf

[2] NTP53x2 - NTAG 5 link, NFC Forum-compliant I^2C bridge, doc.no. 5476xx
https://www.nxp.com/docs/en/data-sheet/NTP53x2.pdf

[3] NTA5332 - NTAG 5 boost, NFC Forum-compliant I^2C bridge for tiny devices, doc.no. 5475xx
https://www.nxp.com/docs/en/data-sheet/NTA5332.pdf

[4] AN11859 - MIFARE Ultralight and NTAG Generating Originality Signature
https://www.docstore.nxp.com/products

[5] AN11350 - NTAG Originality Signature Validation
https://www.nxp.com/confidential/AN11350

[6] AN11808 - ICODE DNA Key initialization, tag/mutual authentication
https://www.docstore.nxp.com/products

[7] AN11807 - ICODE DNA Key diversification, doc.no. 3680xx
https://www.docstore.nxp.com/products

[8] ISO/IEC 29167-10, Information technology — Automatic identification and data capture techniques, Part 10: Crypto suite AES-128 security services for air interface communications, ISO/IEC 29167-10:2015(E)

9 Legal information

9.1 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.

9.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Non-automotive qualified products — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications. In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer. In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages. Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — While NXP Semiconductors has implemented advanced security features, all products may be subject to unidentified vulnerabilities. Customers are responsible for the design and operation of their applications and products to reduce the effect of these vulnerabilities on customer's applications and products, and NXP Semiconductors accepts no liability for any vulnerability that is discovered. Customers should implement appropriate design and operating safeguards to minimize the risks associated with their applications and products.

9.3 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.

9.4 Trademarks

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

I²C-bus — logo is a trademark of NXP B.V.

ICODE and I-CODE — are trademarks 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: 9 January 2020
Document identifier: AN12366
Document number: 530510