AN12366

如何配置NTAG 5的内存和可扩展安全性

第1.0版 — 2020年1月9日
530510

应用笔记
公司公开文件

文档信息

信息	内容
关键词	配置和安全、NTAG 5 switch、NTAG 5 link和NTAG 5 boost、明文密码、AES双向验证
摘要	如何配置NTAG 5的内存以及设置相应安全级别的指南。

修订历史

版本号	日期	说明
第1.0版	2020年1月9日	第一个正式发布的版本

1 缩略语

表1. 缩略语

缩略语	说明
I^2C	IC间通信
IC	集成电路
NFC	近场通信
PACK	密码确认
PWD	密码
VCD	邻近耦合装置
VICC	邻近集成电路卡

2 介绍

本文介绍了如何使用NTAG 5的数据保护功能。NTAG 5具有多种功能来提升数据安全性和隐私性。要利用这些功能，客户需要对系统、IC烧录和读取点操作进行调整。此外，客户还需要遵循安全密码和/或密钥管理规范，确保安装的完整性和安全性的预期改进。

2.1 潜在应用

保护芯片和数据：

- 使用自己的原装产品检查
- 在受保护的只读开放区域使用NDEF消息
- 使用明文密码或AES双向身份验证来保护您的个人设置
- 将内存分为三个独立的受保护区域

3 安全功能

NTAG 5系列有两（2）种安全方案：

1. 明文密码验证模式（与ICODE SLIX2相似）
2. AES身份验证模式，符合ISO/IEC 29167-10标准，使用加密套件AES-128安全服务实现空口通信（与ICODE DNA相似）

表2. NTAG 5的不同安全类型

NTAG 5名称	安全模式	类型
NTAG 5 switch	密码	NTP5210
NTAG 5 link	密码	NTP5312
NTAG 5 link	密码或AES加密套件	NTP5332
NTAG 5 boost	密码或AES加密套件	NTA5332

3.1 身份验证

3.1.1 密码验证

如果通信主机（RF或I^2C）向NTAG 5提供密码（PWD），则可以完成密码验证（32位或64位密码）；如果密码正确，NTAG 5以PACK（密码确认，可配置）来响应。

3.1.2 AES-128验证

AES-128验证提供了一种选择，可以让询问器（VCD）检查对方（VICC）身份是否真实——是否拥有相同的密码或密钥。验证成功后，RF通信将是明文的（没有加密）。如果需要更高的安全性，可以在整个系统层面有效地实现。此外，还可以使用NTAG 5的SRAM（易失性）作为传输层，并结合安全μC将安全手段置于应用层/系统层。

3.2 锁定字节值

为了将用户内存部分永久设置为只读，NTAG 5采用了锁定机制。这个机制可以从两个接口进行配置，而从射频接口只能单向烧录。另外，配置存储器的一些区域也可以被锁定。配置完成后，建议写入适当的锁定条件，并锁定芯片配置字节。

LOCK_BLOCK_ COMMAND_SUPPORTED需要在CONFIG_2字节中设置为1b，才能启用LOCK_BLOCK命令。

NFC锁定模块配置锁的每一位都锁定一个内存模块。SECTION_LOCK“冻结”NFC锁定模块配置。

参见示例[第7.5节]。

3.3 保护功能访问

表3. NTAG 5安全功能

功能	NTAG 5 switch	NTAG 5 link	NTAG 5 link	NTAG 5 boost
类型	NTP52101	NTP5312	NTP5332	NTA5332
锁定模块	有	有	有	有
EAS密码保护	有	有	有	有
AFI密码保护	有	有	有	有
读/写EEPROM密码保护	有	有	有	有
PRIVACY（隐私）密码保护	有	有	有	有
DESTROY（销毁）密码保护	有	有	有	有
标签验证	-	-	有 (1)	有 (1)
双向验证	-	-	有 (1)	有 (1)
否定验证计数器	有	有	有	有
SRAM保护	-	有	有	有
配置区保护	有	有	有	有
会话寄存器保护	有	有	有	有

(1) 将PWD（密码模式）切换为AES模式后可用。

3.4 不同内存区域的保护

用户EEPORM可以分为三个区域。16位PP_AREA_1指针定义了AREA_1的起始位置，从NFC和I^2C的角度来看，AREA_1是相同的块地址。

只有当8位NFC_PP_AREA_0-H模块地址低于PP_AREA_1时，这个部分才会被划分成NFC AREA_0-L和NFC AREA_0-H。由于指针地址为8位，最大分隔可达1 kB。

AREA_0-L和AREA_0-H页面部分可以从RF和I^2C角度来独立定义。此外，RF和I^2C的访问限制也可以不同。要从I^2C角度来划分用户EEPROM，需要相应地设置8位I2C_PP。

这个概念如下图所示。

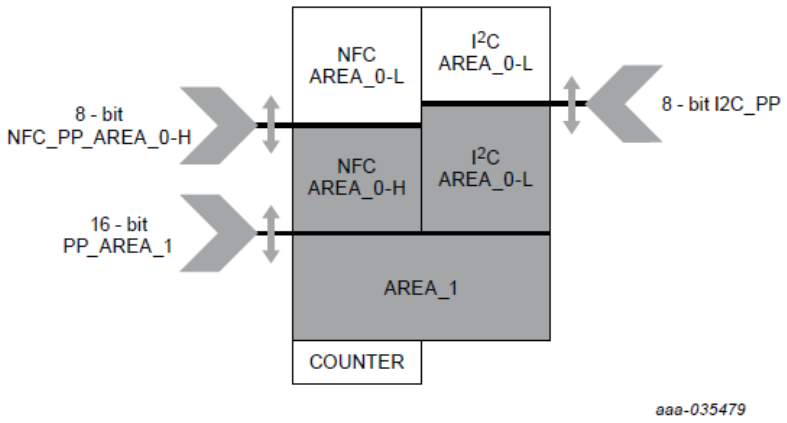


图1. 存储区概念

表4. NTAG 5不同存储区可能采用的保护

存储区域	NFC/RF	I²C
EEPROM	有（NFC_PP_AREA_0-H）	有（I2C_PP）
EEPROM——受限区域	有（PP_AREA_1）	
SRAM	有（密码或验证访问保护）	无
用户配置	有（密码或AES）	有（密码）
寄存器	有（一些）	无

3.5 可重新烧录的原创签名

恩智浦为客户提供了两种方案，一种是锁定恩智浦预烧录的原创签名，另一种是让客户重新烧录并锁定原创签名。

建议按以下步骤生成和重新烧录原创签名：

1. 为secp128r1生成公钥和私钥
2. 使用私钥创建并签署原创签名
3. 用公钥验证原创签名
4. 将签名烧录入集成电路内存
5. 锁定签名

更多详情及所需的微小改动，请参阅[应用笔记]。

有关验证原创签名的更多详情，请参阅[应用笔记]。

4 NFC（RF）方面的安全

4.1 明文密码

身份验证是通过空口明文共享密码来完成的。身份验证成功后，授予相应的访问权限。

可将默认的32位密码长度改为64位密码长度。

4.2 AES模式

它是根据ISO/IEC15693-3 Amendment 4和ISO/IEC29167-10 [国际标准]定义的身份验证模式。使用CBC模式的AES-128加密算法。支持询问器执行两（2）个身份验证程序：

- 标签验证（TAM）
- 双向验证（MAM）

只有NTAG 5 link（NTP5332）和NTAG 5 boost（NTA5332）支持从PWD模式切换到AES模式，在地址3Fh（RF）或103Fh（I^2C）上设置DEV_SEC_CONFIG字节实现。

在身份验证过程中，密钥仅用于加密/解密，从不在空口上交换。

有关数值示例，请参阅[应用笔记]。

4.2.1 标签验证

可通过加密验证证明所用的NTAG 5（终端应用、产品等）是否为原装。标签验证成功后，VCD（询问器）就能证明对应的VICC（NTAG 5）是原装的，可共用相同的密钥。

4.2.1.1 场域内预计只有一个NTAG 5标签

数值示例请参阅[应用笔记]。

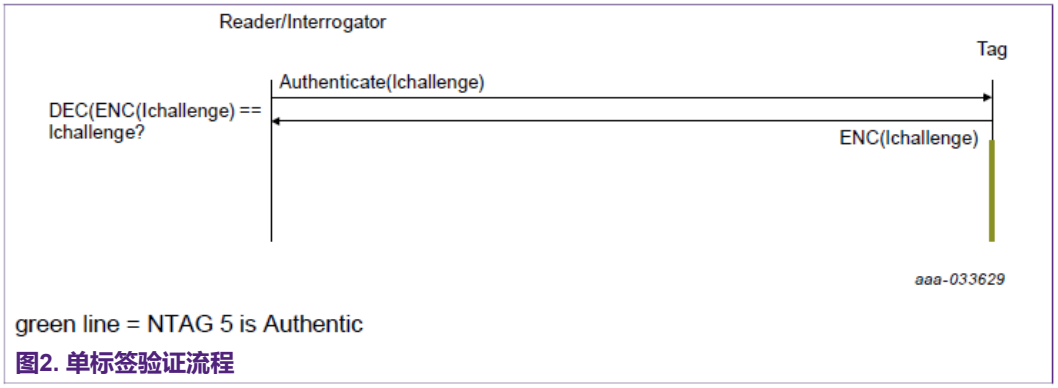


图2. 单标签验证流程

4.2.1.2 场域内预计有多个NTAG 5标签

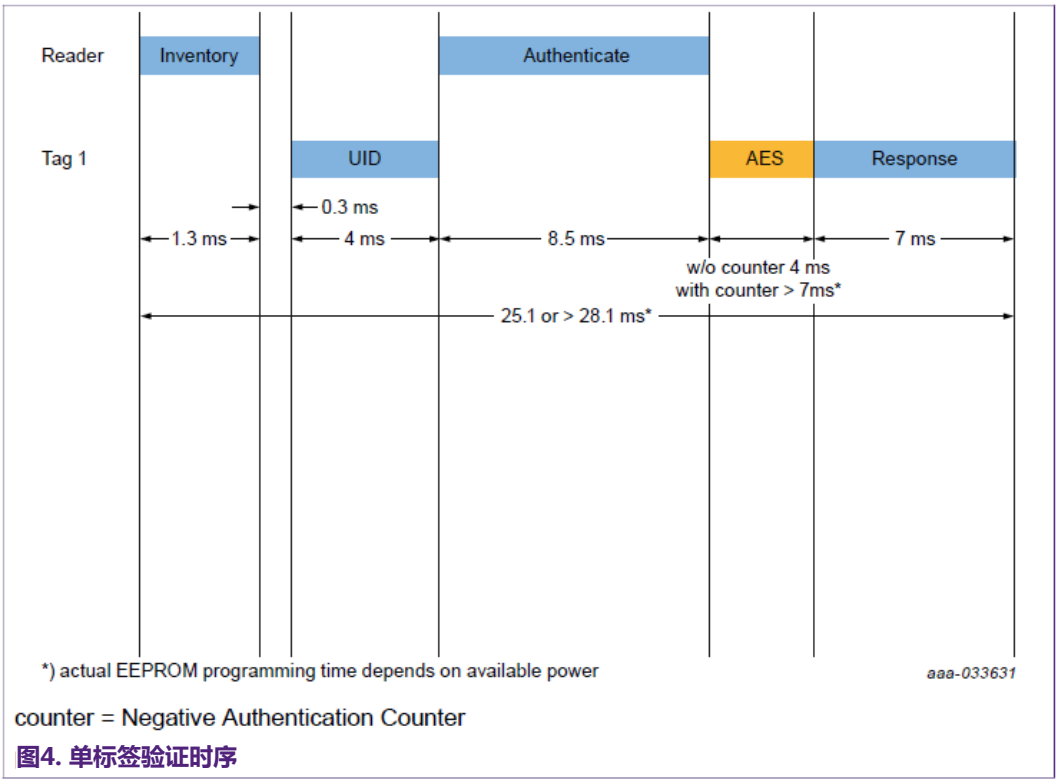
VCD（询问器）向一个NTAG 5或多个NTAG 5发送IChallenge命令。收到有效的CHALLENGE命令后，NTAG 5开始进行加密计算，并将数据存储到其缓冲区。计算完成，NTAG 5将响应有效的READBUFFER命令，并提供加密计算的结果。

在读取特定NTAG 5的缓冲区（READBUFFER）之前，VCD（询问器）决定要寻址（INVENTORY）哪个NTAG 5。

图3. 场域内预计有多个NTAG 5的标签验证

4.2.1.3 时序测量

4.2.1.3.1 单标签验证



counter = Negative Authentication Counter

图4. 单标签验证时序

4.2.1.3.2 多标签验证

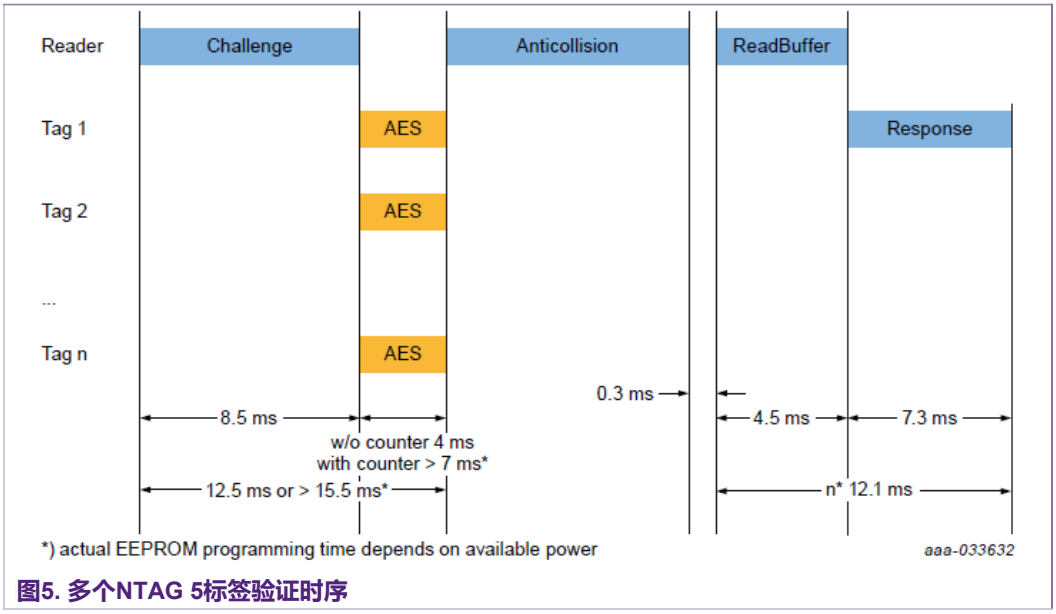


图5. 多个NTAG 5标签验证时序

4.2.2 双向验证

这种验证可防止未经授权的数据访问及未经授权的操作。

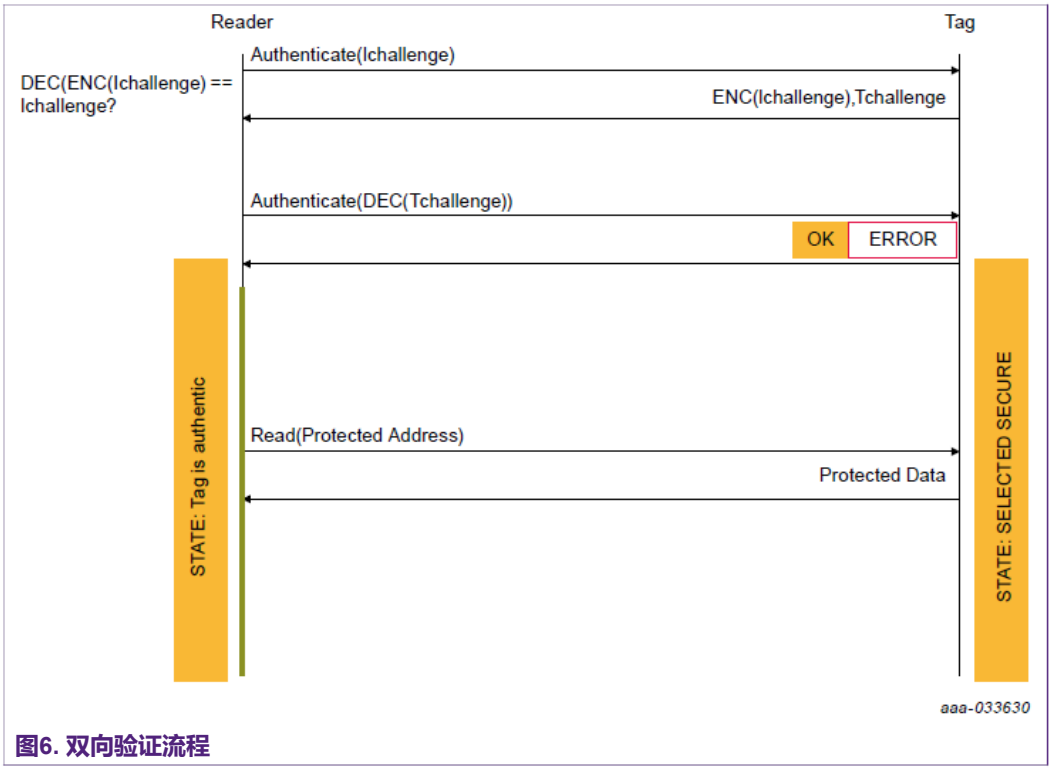


图6. 双向验证流程

5 I²C方面的安全

I²C从机通信可通过明文密码验证进行保护。I²C主机在访问I²C受保护的区域之前，需要通过将相关密码写入相关模块（模块1096h至1099h）来进行验证。

6 密码或密钥生成

NTAG 5使用32位、64位密码和128位AES密钥。这提供了合理的安全级别。

以下是几种生成密码的方法：

1. 客户生成一套用于所有NTAG 5的密码/密钥（例如批量）
2. 客户为每个NTAG 5生成不同的密码/密钥，并将其存储在数据库中。
3. 客户使用IC的UID和安全算法（可自由选择）计算所有IC的不同密码/密钥。（推荐）[应用笔记]

7 示例：场域的安全保护

在下面的示例中，内存的组织方式如下图所示。

- UID：E00401581A003F00
- NDEF – URI记录：

模块[hex]	字节0	字节1	字节2	字节3	区域
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	计数器				

7.1 写入/存储（派生）密码

- 新WRITE PWD（写入密码）值："11223344h"
- WRITE PASSWORD（密码标识符02h）命令代码：B4h（注：也可直接使用WRITE CONFIG写入PWD值）
- 将NTAG置于SELECTED状态或使用Addressed（寻址）模式（命令有效载荷中提供的UID）

操作步骤：

1. 获取随机数
   VCD → VICC: 12 B2 04 (1B B9)
   VICC → VCD: C2 73 + CRC
2. VCD计算XOR_Password[31:0] = 密码[31:0] XOR {Random_Number[15:0], Random_Number[15:0]}。注：默认PWD为00000000h。
   C2 73 C2 73
3. 设置密码（使用默认PWD验证）
   VCD → VICC: 12 B3 04 02 C2 73 C2 73 (6C F8)
   VICC → VCD: 00

4. 写入密码（写入新PWD）

VCD → VICC: 12 B4 04 02 11 22 33 44 (12 1B)

VICC → VCD: 00

7.2 设置保护指针和指针条件

写入保护指针配置：

- NFC_PP_AREA_0-H至（07h）值
- AREA_0_L为：
  - 没有读保护
  - 没有写保护
- AREA_0_H为：
  - 没有读保护
  - 有写保护

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

7.3 芯片安全配置

安全级别可以通过芯片安全配置（DEV_SEC_CONFIG）来设定，并通过两个接口写入。如果芯片安全配置被锁定，则不能再通过任何接口对其进行更新。不同型号的NTAG 5支持不同的IC RF安全特性，NTAG 5 boost (NTA5332)和NTAG 5 link (NTP5332)可以选择AES标签/双向认证或明文密码，而NTAG 5 switch (NTP5210)和NTAG 5 link (NTP5312)只支持明文密码。

从射频角度看，有三种安全级别：

- 32位明文密码
- 64位明文密码
- AES：只适用于NTAG 5 boost(NTA5332)和NTAG 5 link(NTP5332)

安全模式可在DEV_SEC_CONFIG (3Fh)中配置。

从I^2C的角度看，只实现了明文密码保护。

7.4 受限区域配置

受限区域保护指针（PP_AREA_1）设置为60h。受限区域总是受到两个接口的保护。这个区域可由16位地址定义。由于此受限区域具有最高优先级，且与任何L页（AREA_0-L）或H页（AREA_0-H）区域有重叠，这个用户区域被视为受限区域。

VCD → VICC: 02C1043FA500**60**00

执行这个命令后，受限区域会自动受到NFC_PWD5（AREA_1读密码）和NFC_PWD6（AREA_1 写密码）的读写保护。

注意：使用AES安全方案时，这个受限区域的密钥由相关的NFC KeyPrevilegies (NFC_KPx)来定义。

7.5 锁定存储区（只读状态）

将NDEF区域（0000h - 0006h模块）设置为只读，这也可以通过以下两种方式实现：

- LOCK BLOCK命令（也由NFC论坛定义）
- 直接写入Configuration（配置）字节（更快速）

因此需要设置NFC_LOCK_BL0的前7位。

表5. 置位

	位7	位6	位5	位4	位3	位2	位1	位0	[hex]中的字节值
NFC_LOCK_BL0	0	1	1	1	1	1	1	1	7F

操作步骤：

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

8 参考资料

[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 I²C bridge, doc.no. 5476xx
https://www.nxp.com/docs/en/data-sheet/NTP53x2.pdf

[3] NTA5332 - NTAG 5 boost, NFC Forum-compliant I²C 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.

表目录

图目录

目录

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

Date of release: 9 January 2020
Document identifier: AN12366
Document number: 530510