AN13089

NTAG 21x features and hints

Rev. 1.0 — 5 May 2021
654010

Application note
COMPANY PUBLIC

Document information

Information	Content
Keywords	Implementation hints
Abstract	This document presents features and hints for a secured and optimized application development using NTAG 21x products: NTAG 210, NTAG 210μ, NTAG 212, NTAG 213, NTAG 215, NTAG 216, NTAG 213 Tag Tamper, NTAG 213F, NTAG 216F.

Revision history

Revision history

Rev	Date	Description
1.0	20210505	First release

1 Abbreviations

Table 1. Abbreviations

Acronym	Description
AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
C-APDU	Command APDU
CC	Capability Container
CMAC	MAC according to NIST Special Publication 800-38B
CRC	Cyclic Redundancy Check
IC	Integrated Circuit
KDF	Key derivation function
LSB	Lowest Significant Byte
LSb	Lowest Significant bit
MAC	Message Authentication Code
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
NVM	Non-volatile memory
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Card
PRF	Pseudo Random Function
R-APDU	Response APDU (received from PICC)
UID	Unique IDentifier
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

2 Introduction

2.1 Purpose and scope

This application note is intended to describe the features of the NTAG 21x family products.

This application note addresses some security mechanisms which may be used to protect the data stored in the product. For higher degree of security, please consider other products like NTAG 424 DNA or NTAG 426 DNA.

2.2 Disclaimer

Note that whenever terms are used like locking, read-only, fraud protection, security feature and the like, this does not imply that there would never be any attack possible to circumvent the feature.

NTAG 21x is not a security certified product. Depending on the value of the assets that need to be protected, one may consider using Common Criteria certified products with security features that have been demonstrated to resist certain attack potential during certification. (E.g. NTAG 424 DNA, NTAG 426 DNA that have CC enhanced-basic attack potential profile).

2.3 How to use this document

This document contains a collection of hints and features that could be of interest for users, who plan to use the NTAG 21x products.

None of this information is intended to replace any of the relevant data sheets or design guides.

All the numerical examples are just examples, describing the usage of commands and providing reference values to verify any implementation.

Any data, value or cryptogram are expressed here as hex string format if not mentioned otherwise.

<u>In this document, for simplicity sake, NTAG 213 properties are used.</u> Location of configuration bytes, location and granularity of lock bytes may differ between different products - for NTAG 210 [1], NTAG 210µ [4], NTAG 212 [1], NTAG 213 [2], NTAG 215 [2], NTAG 216 [2], NTAG 213 Tag Tamper [3], NTAG 213 F [5], NTAG 216 F [5] please refer to applicable data sheets.

3 NTAG application hints

3.1 Memory features

In addition to the user memory area the NTAG 21x offers the features of an NFC Forum Type 2 Tag defined Capability Container (CC) [1] area and lock bytes to lock the CC and user area. The usage of Lock Bits are described in Section 3.1.1.2.

An NTAG 21x dedicated 4-byte WRITE-command provides a high transaction speed.

3.1.1 Memory organization

The EEPROM memory is organized in pages with 4 bytes per page. The memory organization can be seen in Figure 1 below, the functionality of the different memory sections is described in following topics. Page 03h is the CC page and the default value of the CC bytes on NTAG 213 is E1 10 12 00h. These bytes act as One Time Programmable (OTP) area, they can only be bit-wise modified from 0 to 1 using the WRITE command.

Page Adr		Byte number within a page				
Dec	Hex	0	1	2	3	Description
0	0h	serial number				Manufacturer data and static lock bytes
1	1h	serial number				
2	2h	serial number	internal	lock bytes	lock bytes	
3	3h	Capability Container (CC)				Capability Container
4	4h	user memory				User memory pages
5	5h					
...	...					
38	26h					
39	27h					
40	28h	dynamic lock bytes			RFUI	Dynamic lock bytes
41	29h	CFG 0				Configuration pages
42	2Ah	CFG 1				
43	2Bh	PWD				
44	2Ch	PACK		RFUI		

aaa-008087

For other NTAG 21x products, check respective data sheet Section 10

Figure 1. NTAG 213 Memory organization

3.1.1.1 Capability Container - Recommended implementation

To achieve optimal configuration for the end application, especially in the context of tearing, see also Section 8, one of the following points shall be considered in order of advised recommendation:

1. Set the CC lock bit and all block-locking bits for pages 3 to 15
2. Set the CC lock bit
3. Protect CC bytes by password protection.

1 **O**ne **T**ime **P**rogrammable

3.1.1.2 Static Lock bytes

Page 02h contains the Static Lock byte 0 and 1 which represent the field programmable read-only locking mechanism. Each page from 03h (CC) to 0Fh can be individually locked by setting the corresponding locking bit Lx to logic 1 to prevent further write access. After locking, the corresponding page becomes read-only memory. The three least significant bits of Lock Byte 0 are the Block-locking bits to lock the set values of Lock Bytes.

Note: At configuration (personalization) of the product, it is recommended that all block-locking bits are written twice (with two (2) WRITE commands) to freeze the configuration of Static Lock bytes for page 03h (CC) and the memory area range 04h - 0Fh (04d - 15d). For additional info, see Section 3.1.1.1.

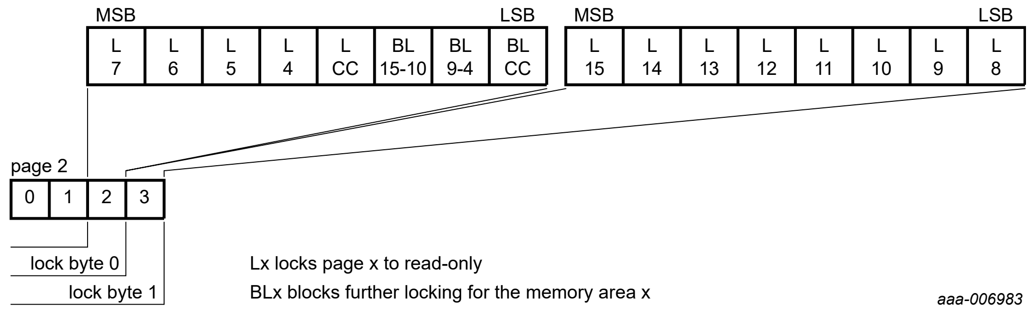


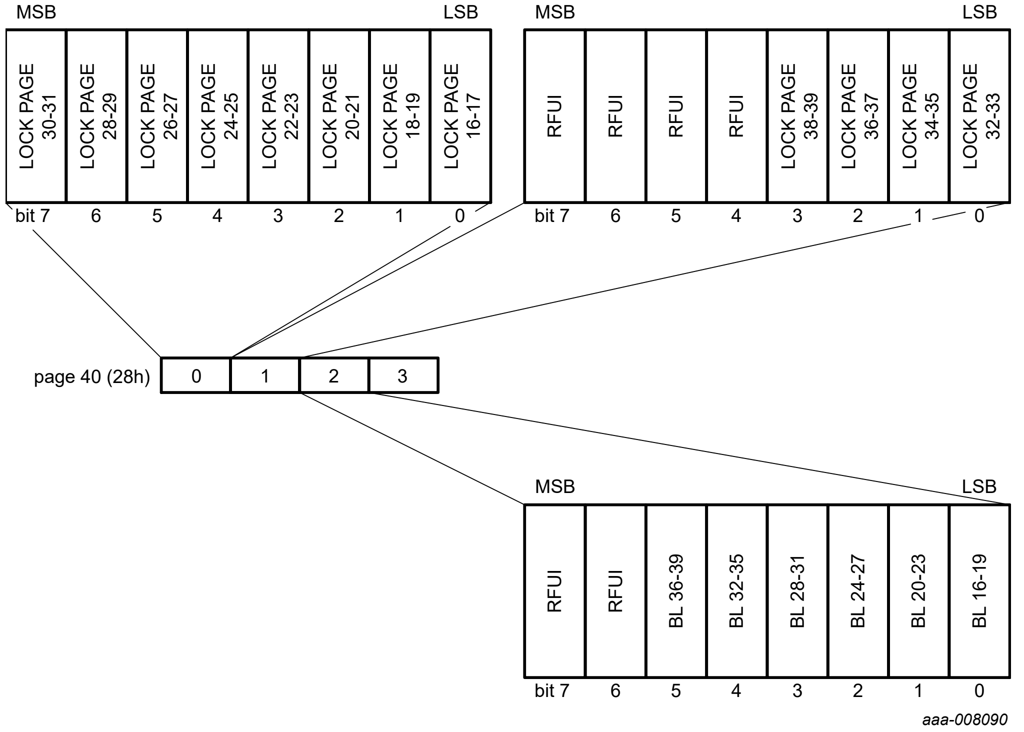
Figure 2. NTAG 213 Static Lock Bytes

In case not all block-locking bits can be set out of the use case, it is recommended to implement an integrity protection e.g. based on truncated MAC Section 3.2.1 over the data stored on locked pages as an additional defense to allow manipulation detection.

3.1.1.3 Dynamic Lock bytes

To lock the memory area pages of NTAG starting at page address 10h (16d) onwards is supported by the Dynamic lock bytes. The granularity of the number of pages locked by the bits depends on the memory area size. Additionally, the block-lock bits lock the configuration of the lock bytes themself.

Note: At configuration (personalization) of the product, after configuring memory area, it is recommended that all block-locking bits are written twice (with two (2) WRITE commands) to freeze the configuration Dynamic Lock bytes.



For other NTAG 21x products, check respective data sheet

Figure 3. NTAG 213 Dynamic Lock bytes

In case not all block-locking bits can be set out of the use case, it is recommended to implement an integrity protection e.g. based on truncated MAC Section 3.2.1 over the data stored on locked pages as an additional defense to allow manipulation detection.

3.1.2 FAST_READ time saving

NTAG 21x introduces the FAST_READ command. The FAST_READ command has a variable frame length depending on the start and end address parameters. The maximum frame length supported by the PCD needs to be taken into account when issuing this command.

The table below shows the comparison in term of timing between READ and FAST_READ. The FAST_READ command is able to speed up the reading compared with the READ command in case of amount of data that is smaller than 4 pages but also bigger than 4 pages. Only in case of 4 pages reading the READ command is faster than the FAST_READ.

Table 2. READ and FAST_READ timing comparison

Command	1 page	4 pages	12 pages	32 pages
READ	2.1 ms	2.1 ms	6.3 ms	16.8 ms
FAST_READ	1.2 ms	3.7 ms	3.7 ms	11.8 ms
FAST_READ Time Gain	0.9 ms	- 1.6 ms	2.6 ms	5 ms

3.2 Proposed security mechanism

NTAG has been designed to support the faster application with the cheapest solution. Therefore, it does not address any security feature except:

- the Unique IDentity (UID),
- the Password protected access
- the Originality Signature Validation based on ECDSA[2]

From the application point of view this means, no cryptographic challenge-response based authentication has to be performed and no key is needed, therefore only limited security is offered.

If required, NTAG 21x can be integrated in an application with additional security by using additional cryptographic protection at the system level. The following two subsections demonstrate how additional integrity protection (see Section 3.2.1) and if needed also confidentiality protection (see Section 3.2.2) of the stored data can be achieved. MIFARE SAM AV3 (secure access module) can be used to store the required key(s) and execute the cryptographic calculations. This SAM module facilitates the system in the following ways:

- The key is stored securely, without being able to be read out.
- The module provides functions for calculation of MAC and encryption (including key diversification if required).
- The cryptographic operations are fast enough for real-time operations.

3.2.1 Integrity of stored data

The content of the NTAG 21x memory lacks guaranteed integrity. To avoid this inconvenience, we propose a security checksum which has to be calculated over the bytes in pages 2 to used memory end and has to be appended with the data. For this purpose, a CMAC (Cipher-based Message Authentication Code) according to the NIST SP800-38B [8] may be a good choice. The complete scheme is shown in Figure 4

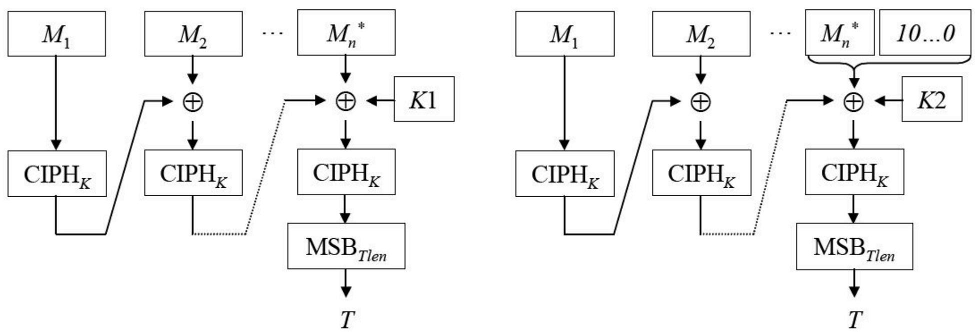


Figure 4. CMAC calculation according to NIST SP800-38. Left side shows input data as a multiple of 16 bytes, right shows padded input data

- The recommended cipher (CIPH) is AES-128.
- Use a secret key (K), which is only known by the reader infrastructure and/or backend.
- The input ($M_1 \ldots M_n$) is the data to be protected concatenated with the UID, e.g. UID || Data.

- Input data blocks (M_n) need to have a size of 16 bytes. If the number of input data bytes is not a multiple of 16, padding is added acc. NIST SP800-38B (80h following by 00s) [8]. This will typically be the case with the UID being 7 bytes and a data page being 4 pages.
- The result of the CMAC calculation is a block of 16 bytes length, which can be truncated to a shorter size as well. Refer to NIST SP800-38B [8] for recommendation on the truncation size, but in general, a size below 8 bytes is not recommended for general applications.

By storing the (truncated) CMAC together with the protected user data in the NTAG 21x user memory, the data is protected against manipulation, as long as the key is kept secret. Including the UID in the MAC calculation, ensures a different MAC is required for each card, even if the protected data is the same. This supports detecting that data has been copied from one NTAG 21x to another. Alternatively, the UID can also be included via a key diversification step, as outlined in Section 3.2.2.

Note that this method does not protect against recording the combination of old content and a valid MAC, and writing it back to the card at a later point of time (i.e. a so-called replay attack). Additional measures can be taken by e.g. including a monotonically increasing counter in the user data and maintaining and checking this in the reader and/or back-end infrastructure. There may also remain residual risks of integrity protected data being copied to a clone or emulator. If more high-level security features, like card-integrated cryptographic support are required, other products of the NTAG IC family can be used in the application, e.g. the NTAG 424 DNA.

3.2.2 Confidentiality of stored data

If the NTAG 21x pages can be read without any authentication, anyone can read the pages using any standard reader. But if the stored data is encrypted with a secured key then these are just some bytes to one who does not have the secret key and information regarding the encryption method. Therefore, by storing the encrypted data in NTAG 21x memory, one can add confidentiality to the data itself.

Note that the password verification method available in the NTAG 21x, does not offer a high security protection. It is an easy and convenient way to prevent unauthorized memory access. However, be aware the even if applied, the data is still exchanged in plain. If a higher level of protection is required, cryptographic methods on application layer can be used to increase the overall system security.

In general, encryption does not provide integrity protection. Therefore, it is recommended to combine encryption still with a MAC, to also avoid manipulation of the data as also discussed in Section 3.2.1. The recommended cipher is AES-128. This leads to the following function, composed of the steps described below.

$$Data_{stored} = f\left(key, data_{origin}, UID\right)$$

A 16-byte Master Key (Mk) has to be defined by the application provider. For each tag, two tag keys are derived from the Master Key (Mk):

- Ck_{MAC} for MACing
- CK_{ENC} for encryption

This can be done using the key diversification of [9] including the UID. Including the UID in the key diversification is another method of ensuring unique MACs for each different tag (even if the protected data is the same), compared to appending the UID to the input data as described in Section 3.2.1. For the encryption, this also ensures different ciphertext is generated for different tags, i.e. not disclosing potentially the same plaintext data is stored. Note that including the UID in the encryption, in a similar way as done for the integrity protection method of the previous section, would result in a bigger ciphertext, consuming more storage space on the tag. Therefore, key diversification is proposed here.

The steps to be followed for the key diversification are indicated in [9] section 2.2 “AES-128 key” where the inputs to the 128-bit AES key diversification are:

- M: the concatenation of a constant with the 7 bytes UID, i.e. respectively:
  - "$CONST_{MAC}$ || UID" for Ck_{MAC}
  - "$CONST_{ENC}$ || UID" for Ck_{ENC}
- K, the 16 bytes AES-128 Master Key (Mk)

And the output is:

- Diversification Key, respectively the 16 bytes AES-128 bits Ck_{MAC} or Ck_{ENC}

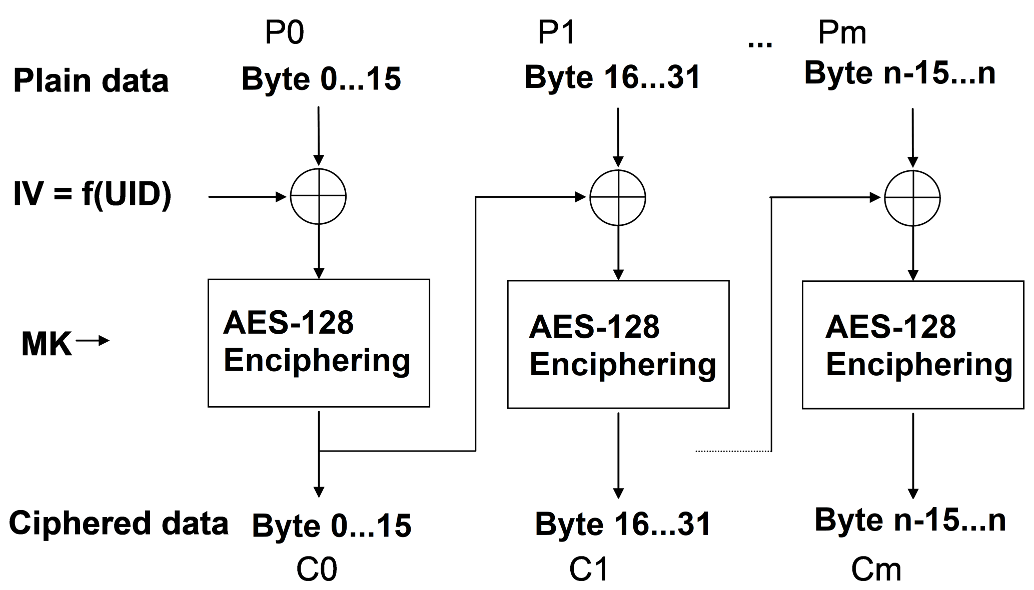
After this step, the plain data is encrypted using the encryption Card Key (Ck_{ENC}) in CBC mode according [NIST SP800-38A] [7].

- Use 16 bytes initial vector (IV) of all ‘00’s, IV= “00...00” (also a random IV can be used. This has the advantage that identical plaintexts would result in a different ciphertext. The drawback is, that the IV needs to be then stored on the tag as well)
- As AES 128 works with 16-byte block wise, organize the data in multiple of 16 by adding one of the padding schemes of [ISO/IEC 9797-1], e.g. Padding Method 1 which results in padding with all zeros ‘00’. As example (‘xx’ is the data bytes):

```
10 padding bytes: xxxxxxxx xxxx0000 00000000 00000000

15 padding bytes: xx000000 00000000 00000000 00000000
```

The complete CBC encryption scheme is shown in the following figures (Figure 5 for encryption and Figure 6 for decryption):



m = (n+1)/16 -1; where m and n are integer
P = plain 16-byte block
C = ciphered 16-byte block

Figure 5. Data encryption scheme

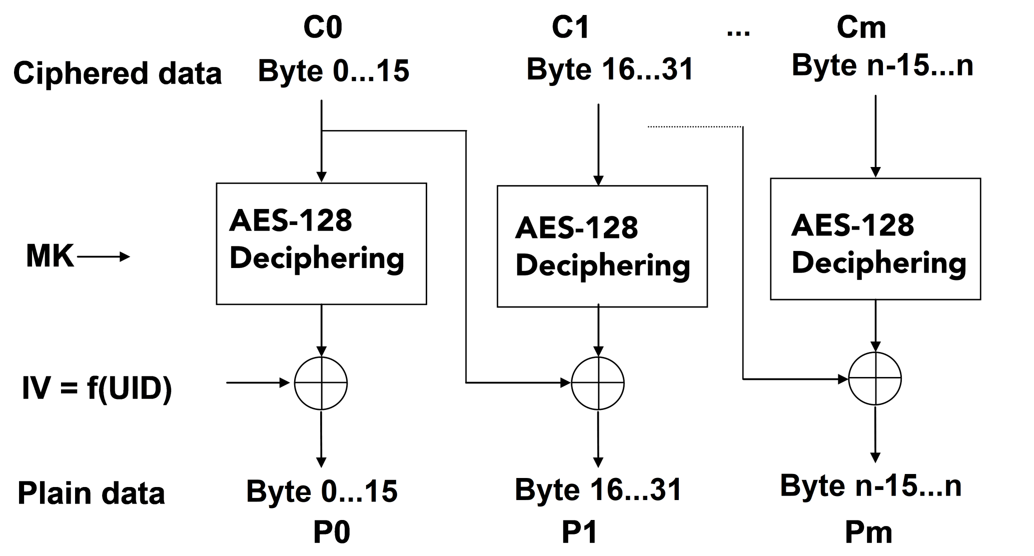


Figure 6. Data decryption scheme

As a final step, a MAC is calculated over the ciphertext. This can be done by applying the CMAC algorithm according [NIST SP800-38B] [8], similar as also used in the previous section, see Figure 4. In this case, Ck_{MAC} is to be applied as the key K, and the ciphertext "C0 … Cn" is the input message M.

Both the ciphertext and the calculated (and eventually truncated) MAC are to be stored on the tag.

4 NFC counter

NTAG 213 (F/TT), NTAG 215 and NTAG 216 (F) are featuring the NFC counter feature.

If the NFC counter is enabled the IC automatically increases the 24-bit NFC counter value by one, triggered by the first valid Read or Fast read command after the NTAG 21x is powered by the RF field. If the ASCII mirror is enabled, the NFC counter value can be mirrored into the user memory where e.g. the URL is stored. If the mobile device reads the URL, the browser will we opened and the UID with the NCF counter value will be sent to the backend system (cloud server).That allows the back-end system to compare the new received counter value based on the UID with the last one stored in the backend. This allows the back-end system to detect a replay of previous messages. In combination of the timestamp, optional location information (e.g. provided by the cell phone) and the difference between the last and the new NFC counter value based on the UID a basic plausibility check can be implemented in the back-end system.

NFC Counter value can be retrieved by:

- Read out from IC by READ_CNT command
- Mirrored automatically to User Memory location (e.g. as a part of NDEF message) Section 5.2

NTAG 42x DNA products have feature, which enables that NFC Counter is dynamically included into cryptographic output - CMAC. Feature is called SUN (Secure Dynamic NNDEF). See [6].

5 ASCII mirroring

This functionality enables NTAG 21x to virtually mirror:

- 7 byte UID
- 3 byte NFC counter value
- 4 byte Tag Tamper message

over the physical memory of the IC in ASCII code. This mirror can be part of NDEF Message Record as shown below. On the READ or FAST READ command to the involved user memory pages, NTAG 21x responds with the virtual memory content of the UID, NFC counter value and Tag Tamper message (if available on the product and enabled) in ASCII code.

Note: If ASCII mirroring is enabled (MIRROR_EN = 1b), UID and NFC Counter are always mirrored together with "x" as separator character. Means that e.g. NFCCounter mirror cannot be disabled, keeping UID enabled.

Block [hex]	Byte 0	Byte 1	Byte 3	Byte 4	ASCII
00	04	AA	2B	0D	(UID)
01	D2	33	57	80	(UID)
02	36	48	00	00	(BCC1)
03	E1	10	12	00	(CC)
04	01	03	A0	0C	….
05	34	03	3E	D1	4.>.
06	01	3A	55	04	.
07	6E	74	61	67	ntag
08	2E	6E	78	70	.nxp
09	2E	63	6F	6D	.com
0A	2F	32	32	78	/22x
0B	3F	6D	3D	30	?m=0
0C	31	30	32	30	1020
0D	33	30	34	30	3040
0E	35	39	36	30	5060
0F	37	78	36	35	7x65
10	34	33	32	31	4321
11	78	30	31	30	x010
12	32	30	33	30	2030
13	34	30	35	30	4050
14	36	30	37	30	6070
15	38	FE	00	00	8
.	00	00	00	00	

Figure 7. Physically programmed EEPROM memory

Block [hex]	Byte 0	Byte 1	Byte 3	Byte 4	ASCII
00	04	AA	2B	0D	(UID)
01	D2	33	57	80	(UID)
02	36	48	00	00	(BCC1)
03	E1	10	12	00	(CC)
04	01	03	A0	0C	….
05	34	03	3E	D1	4.>.
06	01	3A	55	04	.
07	6E	74	61	67	ntag
08	2E	6E	78	70	.nxp
09	2E	63	6F	6D	.com
0A	2F	32	32	78	/22x
0B	3F	6D	3D	30	?m=0
0C	34	41	41	32	4AA2
0D	42	44	32	33	BD23
0E	33	35	37	38	3578
0F	30	78	30	30	0x00
10	30	30	30	31	0001
11	78	42	31	38	xB18
12	38	41	43	36	8AC6
13	46	36	39	31	F691
14	34	30	42	39	40B9
15	32	FE	00	00	2
.	00	00	00	00	

Figure 8. Virtual content overlay

NDEF Message - Record 1. URI Records of:

- Physically programmed EEPROM: https://ntag.nxp.com/22x?m=01020304050607x654321x0102030405060708
- Virtual overlaid content: https://ntag.nxp.com/22x?m=04AA2BD2335780x000001xB188AC6F69140B92

5.1 UID ASCII mirror function

With MIRROR_EN enabled, ISO14443 7-Byte UID is mirrored into User EEPROM memory. Values are HEX values of ASCII characters mirrored when NFC interface reader does first READ (or FAST_READ) command during RF ON session. Location of mirror start can be configured by setting MIRROR_PAGE and MIRROR_BYTE.

NFC Forum compatible interface reads NDEF message from the tag and converts it from HEX to ASCII automatically.

Block [hex]	Byte 0	Byte 1	Byte 3	Byte 4	ASCII
00	04	AA	2B	0D	(UID)
01	D2	33	57	80	(UID)
02	36	48	00	00	(BCC1)
03	E1	10	12	00	(CC)
04	01	03	A0	0C	….
05	34	03	3E	D1	4.>.
06	01	3A	55	04	.
07	6E	74	61	67	ntag
08	2E	6E	78	70	.nxp
09	2E	63	6F	6D	.com
0A	2F	32	32	78	/22x
0B	3F	6D	3D	30	?m=0
0C	34	41	41	32	4AA2
0D	42	44	32	33	BD23
0E	33	35	37	38	3578
0F	30	.	.	.	0...
.	.	.	.	.	.

Figure 9. UID ASCII mirror

NFC Forum reader parses read NDEF URI Record content to OS as:

https://ntag.nxp.com/22x?m=04AA2BD2335780... (rest)

5.2 NFC counter ASCII mirror function

The 24-bit NFC Counter is located in dedicated memory location, which can be accessed by READ_CNT command. Value of NFC Counter can be mirrored (if MIRROR_EN set) over User memory EEPROM in MSB order as HEX equivalent to ASCII number.

Block [hex]	Byte 0	Byte 1	Byte 3	Byte 4	ASCII
..	.	.	.	.	(....)
0F	.	78	30	30	0x00
10	30	30	30	31	0001
11	78	.	.	.	xB18
..	.	.	.	.	....

NFCCount.	00	00	01	RFUI
	MSB		LSB	

Figure 10. NFC Counter ASCII mirror

NFC Forum reader parses read NDEF URI Record content to OS as:

https://ntag.nxp.com/22x?m=04AA2BD2335780x000001...

6 Authentication

6.1 NTAG password and PACK

The NTAG provides a password authentication to limit a part of the memory area for being accessed either in writing or reading and writing [2].

Although the password verification method available in NTAG 21x does not offer a high security protection, it can be as well (besides the Originality signature check described in [10]) used to verify the originality of the tag. Please note that the password and the PACK are sent in plain and this needs to be considered when assessing the system security whether this is sufficient for the assets to be protected in the targeted application.

6.1.1 Password and PACK diversification

In case the password authentication is used, it is recommended to diversify the Password and the PACK to reduce the risk of compromise password/PACK. The diversification is done similarly to the key diversification described in [9] section 2.2 “AES-128 Key”. In this case, the following items are defined:

- K: a 16 bytes AES 128 bits Master Key
- M: the 7 bytes UID of the NTAG, also called diversification inputs
- CMAC: the output from the 128-bits AES key Diversification called “diversified key” as indicated in Section 2.2 and Figure 2 of [9]
- Dp: diversified Password
- Dpack: diversified PACK

The figure below describes the diversification scheme and how to obtain the diversified Password and PACK.

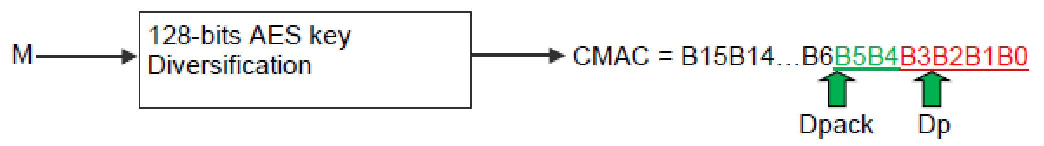


Figure 11. Example of diversification procedure

From the Figure 11, the Dp is obtained from the 4 LSB of the CMAC indicated as B3…B0, and the Dpack is derived from the next 2 bytes indicated as B5B4.

6.1.2 Password authentication command flow

ISO14443-3 activation is needed upfront.

Table 3. Command PWD_AUTH

Step	Command		Data Message
1	Password (shall be diversified as recommended in Section 6.1.1)	=	00000000
3	Command: PWD_AUTH	=	1B
4	Arg	=	00
5	IV	=	00000000000000000000000000000000

Table 3. Command PWD_AUTH...*continued*

Step	Command		Data Message
6	PWD_AUTH with password	>	1B00000000
7	R-APDU PACK[1] (shall be diversified as recommended in Section 6.1.1)	<	0000

1 - PACK response is configurable/programmable

6.2 Negative Authentication Counter

To limit the risk of brute force attacks, a feature of Negative Authentication Counter can be enabled by setting AUTH_LIM to different value than 000h.

7 NTAG anti-cloning based on Originality check

The NTAG supports the originality function based on a 32-byte ECC signature [2]. The application note [10] describes how to validate the signature (retrieved from the NTAG using the READ_SIG command) using the NTAG UID (Unique IDentifier) and the ECC public key provided by NXP Semiconductors.

The purpose of originality check during (pre-)personalization is to protect customer investments by identifying mass penetration of non-NXP originated NTAG 21x ICs into an infrastructure. As individual signatures can still be copied, it does not completely prevent hardware copy or emulation of individual NTAG 21x ICs. As such, a valid signature is not a full guarantee. Therefore, this signature validation should be complemented with a check to detect if multiple ICs with the same UID are being introduced in the system.

8 NTAG 21x anti-tearing implementation

The NTAG 21x implements anti-tearing for OTP, lock bits and counters. This means that in case of a tear-off event either the old value or the new (just written) value is present. This section describes what measures a NTAG 21x application needs to implement in order to ensure the best tear-off protection for the user data pages.

For the tearing application implementation, 2 memory areas having the same size are needed see Figure 12.

Figure 12. Tearing application implementation

The application data is stored in 2 memory locations. The application data also contains a timestamp indicated in white and a CMAC (that can be calculated as indicated in Section 3.2). Every time a new update is needed i.e. new data has to be written, only the set of data with the older timestamp is updated. The CMAC is added to guarantee the integrity of the written application data.

In particular, the Figure 12 shows a typical update of the Application Data done on the older Application Data set (timestamp = t-1). As soon as the new application data is written, the timestamp is updated (timestamp = t+1) and the CMAC is also written.

If the update operation fails due to a tearing event and the application data becomes corrupted, this can be recognized based on the failure of the CMAC validation. In any case, the NTAG 21x either contains the latest updated application data (timestamp = t+1) or the previous one (timestamp = t).

8.1 Recommended system implementations of tearing supported features

NTAG 21x supports anti-tearing support for NFC counter, CC area and Lock bits that may occur during normal operation in the field. Security researches continuously advise the industry by publishing new attack vectors to advocate for higher secure products and implementation of system level countermeasures. It has been demonstrated that applying tearing events in specific sequences can intentionally alter the data of the NFC counter, CC bits and Lock bits. Therefore, it is important that additional measures are considered depending on the configuration and use case.

Table 4. System level countermeasures

Tearing supported features of NTAG 21x	Product and system level recommendation
NFC Counter	1. Use Backend fraud detection e.g. online check by storing latest NFC counter value based on UID. 2. Store the latest NFC counter value based on UID in the reading device and reject the number which appears to be replayed. If application allows it, add a mechanism to synchronize reading devices (e.g. once a day) to reduce time window for replays.
Capability Container (CC) *(One-Time-Programmable bits)*	1. Set the CC lock bit and all block-locking bits for page 3 to 15 **twice** 2. Set the CC lock bit 3. Protect CC bytes with password protection (AUTH0)
Lock bits *(represent the field programmable read-only locking mechanism)*	1. Set all block-locking bits **twice** 2. Protect lock bits by password protection

The proposed countermeasures can be applied on IC by setting all block-locking bits and use of password. Of importance is also, that the programming of the block-locking bits is done **twice** to ensure a permanent lock. The reason for this is, that it makes sure also the internal backup page is updated correctly.

System level countermeasures in general have an impact on the infrastructure (reader and backend system) and can require the storage of some extra information in the contactless tag to increase te system security overall. In general these countermeasures, e.g. calculation of a CMAC over protected data can be implemented on any tag type, unless the storage capacity of the tag is too low to store all extra data.

9 NTAG coil design hints

The NTAG chip is available in two versions: input capacitance of approximately 17 pF or input capacitance of approximately 50 pF. For a complete coil design, refer to the Application Note - NTAG Antenna Design Guide [11].

10 References

[1] NTAG 210/212 - NFC Forum Type 2 Tag compliant IC with 48/128 bytes user memory, Rev. 3.0 — 14 March 2013, DocStore no. 2423xx https://www.nxp.com/docs/en/data-sheet/NTAG210_212.pdf

[2] NTAG 213/215/216 - NFC Forum Type 2 Tag compliant IC with 144/504/888 bytes user memory, Rev. 3.2 — 2 June 2015, DocStore no 2653xx https://www.nxp.com/docs/en/data-sheet/NTAG213_215_216.pdf

[3] NTAG 213 TT - NFC T2T compliant IC with Tag Tamper feature, Rev. 1.1 — 28 March 2017, DocStore no. 3983xx https://www.nxp.com/docs/en/data-sheet/NT2H1311TT.pdf

[4] NTAG 210µ - NFC Forum Type 2 Tag compliant IC with 48 bytes user memory, Rev. 3.0 — 7 September 2016, DocStore no. 3439xx https://www.nxp.com/docs/en/data-sheet/NT2L1001_NT2H1001.pdf

[5] NTAG 213F/216F - NFC Forum Type 2 Tag compliant IC with 144/888 bytes user memory and field detection, Rev. 3.6 — 28 September 2015, DocStore no. 2622xx https://www.nxp.com/docs/en/data-sheet/NTAG213F_216F.pdf

[6] NTAG 424 DNA - Secure NFC T4T compliant IC, Rev 3.0 — 31 January 2019, DocStore no. 4655xx https://www.nxp.com/docs/en/data-sheet/NT4H2421Gx.pdf

[7] NIST Special Publication 800-38A, National Institute of Standards and Technology (NIST). Recommendation for BlockCipher Modes of Operation https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

[8] NIST Special Publication 800-38B, National Institute of Standards and Technology (NIST). Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38B.pdf

[9] AN10922 - Symmetric key diversifications, Rev. 2.2 — 2. July 2019, DocStore no.1653xx

[10] AN11350 - NTAG Originality Signature Validation - Rev. 1.2 — 22 August 2017, DocStore no. 2604xx

[11] AN11276 - NTAG Antenna Design Guide - Rev. 1.8 — 23 October 2018, DocStore no. 2421xx

11 Appendix

11.1 Worked out example of proposed security mechanism

An example application flow diagram is shown in the following:

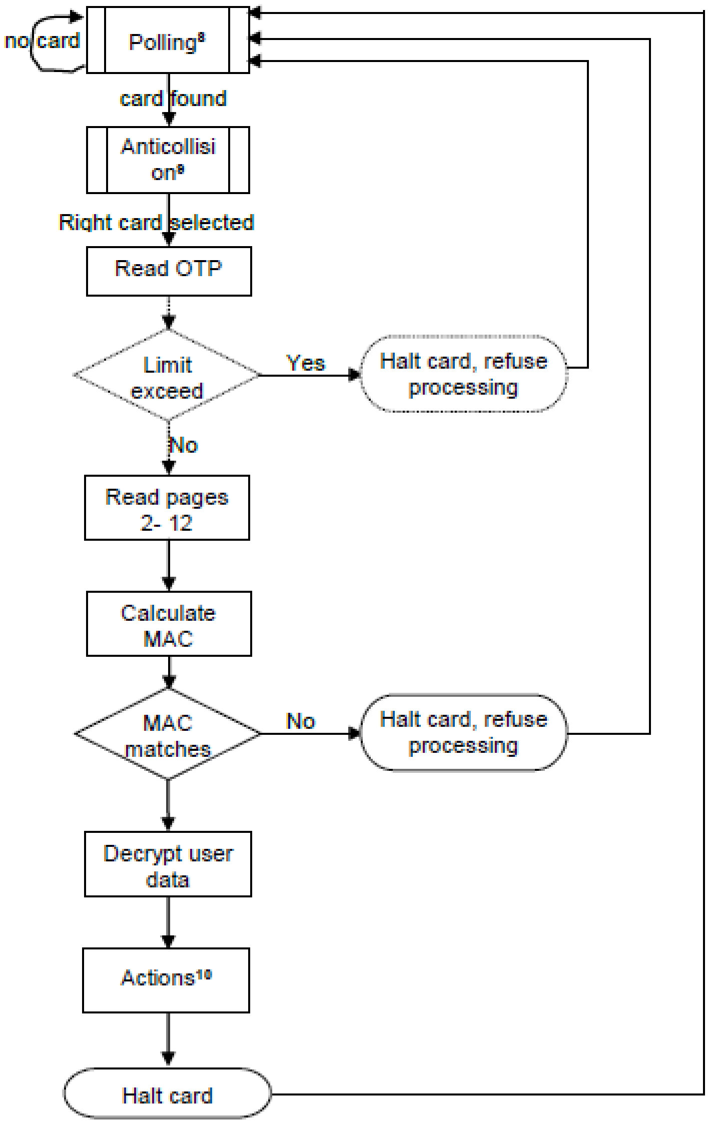


Figure 13. Example application flow diagram

Dotted blocks may be avoided, if the CC bytes are not used.

[8] Pre-defined process for card detection, reader sends always REQA and checks if there is any answer.

[9] Standard anti-collision ISO/IEC 14443-3, which includes the selection of the right card (also from the multiple cards).

[10] If CC or any memory content is updated, MAC has to be recalculated and rewritten.

12 Legal information

12.1 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.

12.2 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.

12.3 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.

12.4 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.

MIFARE Plus — is a trademark of NXP B.V.

MIFARE Ultralight — is a trademark of NXP B.V.

MIFARE Classic — is a trademark of NXP B.V.

NTAG — is a trademark of NXP B.V.

NXP — wordmark and logo are trademarks of NXP B.V.

Tables

Figures

Contents

Date of release: 5 May 2021
Document identifier: AN13089
Document number: 654010