Chipsmall Limited consists of a professional team with an average of over 10 year of expertise in the distribution of electronic components. Based in Hongkong, we have already established firm and mutual-benefit business relationships with customers from,Europe,America and south Asia,supplying obsolete and hard-to-find components to meet their specific needs.

With the principle of “Quality Parts,Customers Priority,Honest Operation,and Considerate Service”,our business mainly focus on the distribution of electronic components. Line cards we deal with include Microchip,ALPS,ROHM,Xilinx,Pulse,ON,Everlight and Freescale. Main products comprise IC,Modules,Potentiometer,IC Socket,Relay,Connector.Our parts cover such applications as commercial,industrial, and automotives areas.

We are looking forward to setting up business relationship with you and hope to provide you with the best service and solution. Let us make a better world for our industry!

Contact us

Tel: +86-755-8981 8866 Fax: +86-755-8427 6832
Email & Skype: info@chipsmall.com Web: www.chipsmall.com
Address: A1208, Overseas Decoration Building, #122 Zhenhua RD., Futian, Shenzhen, China

NTAG213/215/216

NFC Forum Type 2 Tag compliant IC with 144/504/888 bytes user memory

Rev. 3.2 — 2 June 2015
265332

Product data sheet
COMPANY PUBLIC

1. General description

NTAG213, NTAG215 and NTAG216 have been developed by NXP Semiconductors as standard NFC tag ICs to be used in mass market applications such as retail, gaming and consumer electronics, in combination with NFC devices or NFC compliant Proximity Coupling Devices. NTAG213, NTAG215 and NTAG216 (from now on, generally called NTAG21x) are designed to fully comply to NFC Forum Type 2 Tag (Ref. 2) and ISO/IEC14443 Type A (Ref. 1) specifications.

Target applications include Out-of-Home and print media smart advertisement, SoLoMo applications, product authentication, NFC shelf labels, mobile companion tags.

Target use cases include Out-of-Home smart advertisement, product authentication, mobile companion tags, Bluetooth or Wi-Fi pairing, electronic shelf labels and business cards. NTAG21x memory can also be segmented to implement multiple applications at the same time.

Thanks to the high input capacitance, NTAG21x tag ICs are 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 NTAG21x are tailored to meet the requirements of inlay and tag manufacturers.

1.1 Contactless energy and data transfer

Communication to NTAG21x can be established only when the IC is connected to an antenna. Form and specification of the coil is out of scope of this document.

When NTAG21x is positioned in the RF field, the high speed RF communication interface allows the transmission of the data with a baud rate of 106 kbit/s.

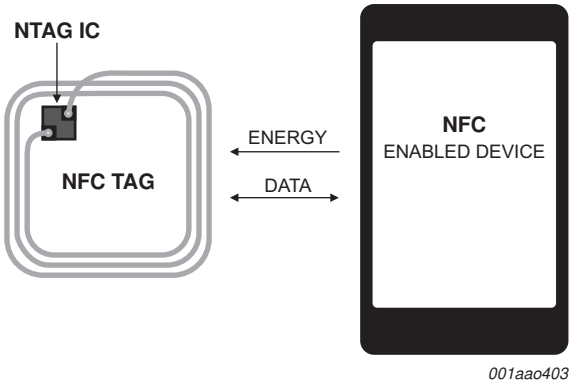


Fig 1. Contactless system

1.2 Simple deployment and user convenience

NTAG21x offers specific features designed to improve integration and user convenience:

- The fast read capability allows to scan the complete NDEF message with only one FAST_READ command, thus reducing the overhead in high throughput production environments
- The improved RF performance allows for more flexibility in the choice of shape, dimension and materials
- The option for 75 μm IC thickness enables the manufacturing of ultrathin tags, for a more convenient integration in e.g. magazines or gaming cards.

1.3 Security

- Manufacturer programmed 7-byte UID for each device
- Pre-programmed Capability container with one time programmable bits
- Field programmable read-only locking function
- ECC based originality signature
- 32-bit password protection to prevent unauthorized memory operations

1.4 NFC Forum Tag 2 Type compliance

NTAG21x IC provides full compliance to the NFC Forum Tag 2 Type technical specification (see Ref. 2) and enables NDEF data structure configurations (see Ref. 3).

1.5 Anticollision

An intelligent anticollision function allows to operate more than one tag in the field simultaneously. The anticollision algorithm selects each tag individually and ensures that the execution of a transaction with a selected tag is performed correctly without interference from another tag in the field.

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

2. Features and benefits

- Contactless transmission of data and supply energy
- Operating frequency of 13.56 MHz
- Data transfer of 106 kbit/s
- Data integrity of 16-bit CRC, parity, bit coding, bit counting
- Operating distance up to 100 mm (depending on various parameters as e.g. field strength and antenna geometry)
- 7-byte serial number (cascade level 2 according to ISO/IEC 14443-3)
- UID ASCII mirror for automatic serialization of NDEF messages
- Automatic NFC counter triggered at read command
- NFC counter ASCII mirror for automatic adding the NFC counter value to the NDEF message
- ECC based originality signature
- Fast read command
- True anticollision
- 50 pF input capacitance

2.1 EEPROM

- 180, 540 or 924 bytes organized in 45, 135 or 231 pages with 4 bytes per page
- 144, 504 or 888 bytes freely available user Read/Write area (36, 126 or 222 pages)
- 4 bytes initialized capability container with one time programmable access bits
- Field programmable read-only locking function per page for the first 16 pages
- Field programmable read-only locking function above the first 16 pages per double page for NTAG213 or per 16 pages for NTAG215 and NTAG216
- Configurable password protection with optional limit of unsuccessful attempts
- Anti-tearing support for capability container (CC) and lock bits
- ECC supported originality check
- Data retention time of 10 years
- Write endurance 100.000 cycles

3. Applications

- Smart advertisement
- Goods and device authentication
- Call request
- SMS
- Call to action
- Voucher and coupons
- Bluetooth or Wi-Fi pairing
- Connection handover
- Product authentication
- Mobile companion tags
- Electronic shelf labels
- Business cards

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

4. Quick reference data

Table 1. Quick reference data

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
C_i	input capacitance		[1]	-	50.0	-	pF
f_i	input frequency			-	13.56	-	MHz
EEPROM characteristics							
t_{ret}	retention time	T_{amb} = 22 °C		10	-	-	years
$N_{endu(W)}$	write endurance	T_{amb} = 22 °C		100000	-	-	cycles

[1] LCR meter, T_{amb} = 22 °C, f_i = 13.56 MHz, 2 V RMS.

5. Ordering information

Table 2. Ordering information

Type number	Package		
	Name	Description	Version
NT2H1311G0DUF	FFC Bump	8 inch wafer, 75 μm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 144 bytes user memory, 50 pF input capacitance	-
NT2H1311G0DUD	FFC Bump	8 inch wafer, 120 μm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 144 bytes user memory, 50 pF input capacitance	-
NT2H1311G0DA8	MOA8	plastic lead less module carrier package; 35 mm wide tape,144 bytes user memory, 50 pF input capacitance	SOT500-4
NT2H1511G0DUF	FFC Bump	8 inch wafer, 75 μm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 504 bytes user memory, 50 pF input capacitance	-
NT2H1511G0DUD	FFC Bump	8 inch wafer, 120 μm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 504 bytes user memory, 50 pF input capacitance	-
NT2H1511G0DA8	MOA8	plastic lead less module carrier package; 35 mm wide tape, 504 bytes user memory, 50 pF input capacitance	SOT500-4
NT2H1611G0DUF	FFC Bump	8 inch wafer, 75 μm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 888 bytes user memory, 50 pF input capacitance	-
NT2H1611G0DUD	FFC Bump	8 inch wafer, 120 μm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 888 bytes user memory, 50 pF input capacitance	-
NT2H1611G0DA8	MOA8	plastic lead less module carrier package; 35 mm wide tape, 888 bytes user memory, 50 pF input capacitance	SOT500-4

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

6. Block diagram

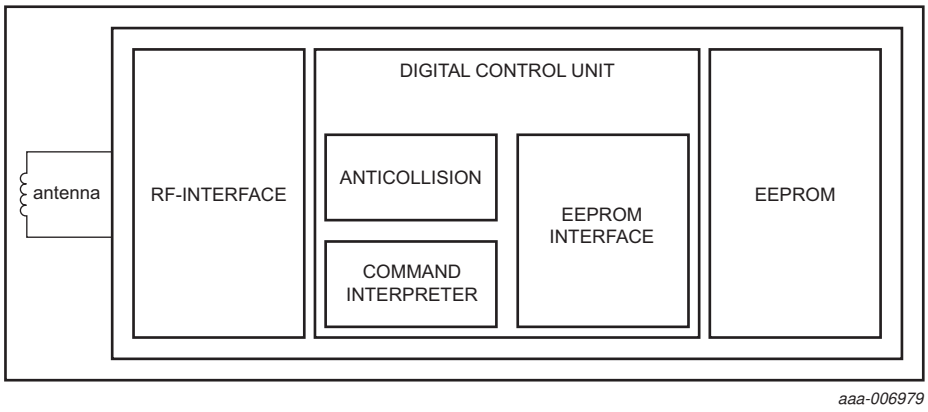


Fig 2. Block diagram of NTAG213/215/216

7. Pinning information

7.1 Pinning

The pinning of the NTAG213/215/216 wafer delivery is shown in section “Bare die outline” (see Section 15).

The pinning of the NTAG213/215/216 MOA8 module is shown in Figure 3.

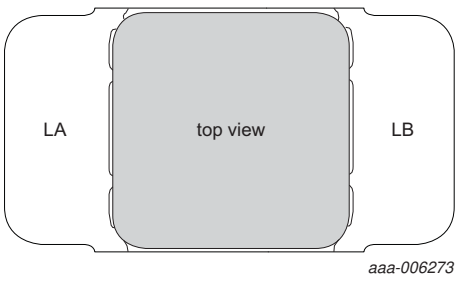


Fig 3. Pin configuration for SOT500-4 (MOA8)

Table 3. Pin allocation table

Pin	Symbol	
LA	LA	Antenna connection LA
LB	LB	Antenna connection LB

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

8. Functional description

8.1 Block description

NTAG21x ICs consist of a 180 (NTAG213), 540 bytes (NTAG215) or 924 bytes (NTAG216) EEPROM, RF interface and Digital Control Unit (DCU). Energy and data are transferred via an antenna consisting of a coil with a few turns which is directly connected to NTAG21x. No further external components are necessary. Refer to Ref. 4 for details on antenna design.

- RF interface:
  - modulator/demodulator
  - rectifier
  - clock regenerator
  - Power-On Reset (POR)
  - voltage regulator
- Anticollision: multiple cards may be selected and managed in sequence
- Command interpreter: processes memory access commands supported by the NTAG21x
- EEPROM interface
- NTAG213 EEPROM: 180 bytes, organized in 45 pages of 4 byte per page.
  - 26 bytes reserved for manufacturer and configuration data
  - 34 bits used for the read-only locking mechanism
  - 4 bytes available as capability container
  - 144 bytes user programmable read/write memory
- NTAG215 EEPROM: 540 bytes, organized in 135 pages of 4 byte per page.
  - 26 bytes reserved for manufacturer and configuration data
  - 28 bits used for the read-only locking mechanism
  - 4 bytes available as capability container
  - 504 bytes user programmable read/write memory
- NTAG216 EEPROM: 924 bytes, organized in 231 pages of 4 byte per page.
  - 26 bytes reserved for manufacturer and configuration data
  - 37 bits used for the read-only locking mechanism
  - 4 bytes available as capability container
  - 888 bytes user programmable read/write memory

8.2 RF interface

The RF-interface is based on the ISO/IEC 14443 Type A standard.

During operation, the NFC device generates an RF field. The RF field must always be present (with short pauses for dat communication) as it is used for both communication and as power supply for the tag.

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

For both directions of data communication, there is one start bit at the beginning of each frame. Each byte is transmitted with an odd parity bit at the end. The LSB of the byte with the lowest address of the selected block is transmitted first. The maximum length of a NFC device to tag frame is 163 bits (16 data bytes + 2 CRC bytes = 16×9 + 2×9 + 1 start bit). The maximum length of a fixed size tag to NFC device frame is 307 bits (32 data bytes + 2 CRC bytes = 32× 9 + 2 × 9 + 1 start bit). The FAST_READ command has a variable frame length depending on the start and end address parameters. The maximum frame length supported by the NFC device needs to be taken into account when issuing this command.

For a multi-byte parameter, the least significant byte is always transmitted first. As an example, when reading from the memory using the READ command, byte 0 from the addressed block is transmitted first, followed by bytes 1 to byte 3 out of this block. The same sequence continues for the next block and all subsequent blocks.

8.3 Data integrity

Following mechanisms are implemented in the contactless communication link between NFC device and NTAG to ensure very reliable data transmission:

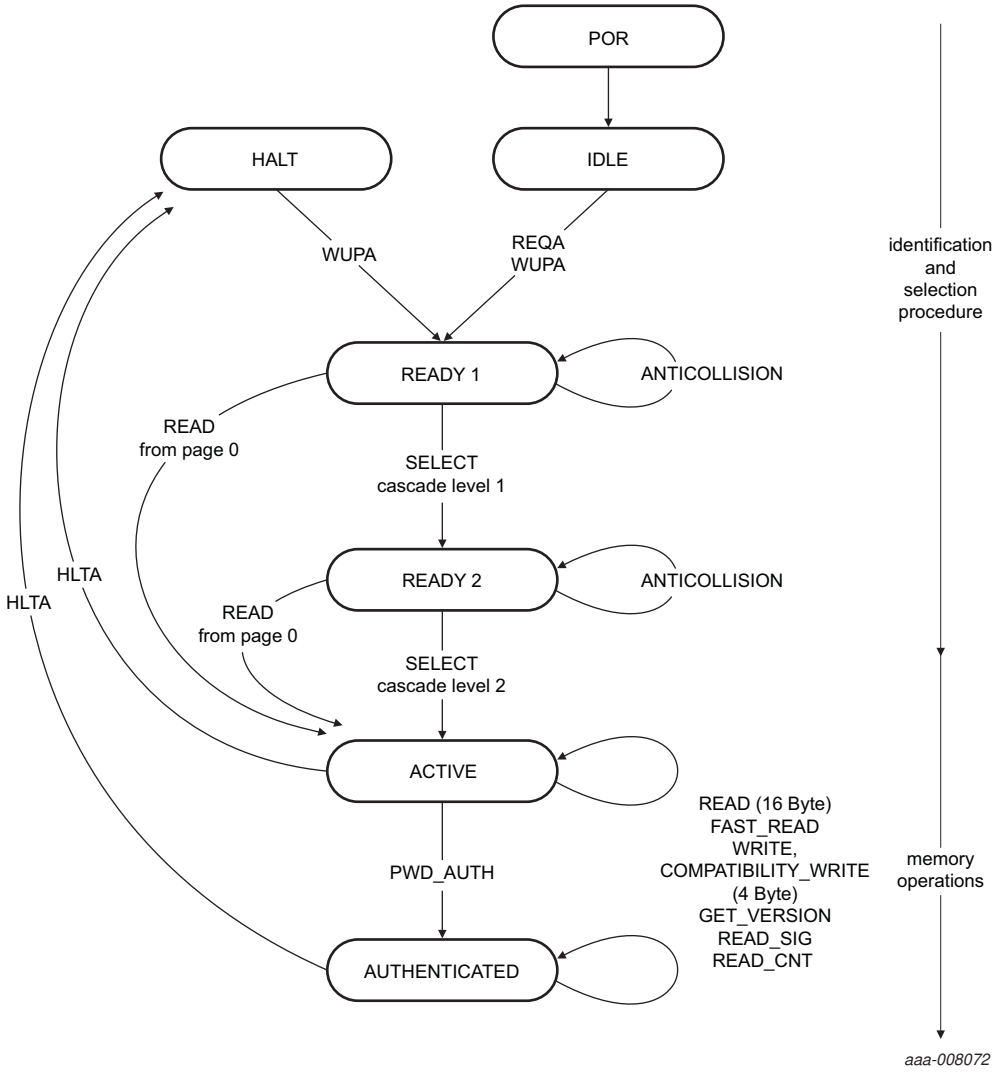
- 16 bits CRC per block
- parity bits for each byte
- bit count checking
- bit coding to distinguish between “1”, “0” and “no information”
- channel monitoring (protocol sequence and bit stream analysis)

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

8.4 Communication principle

The commands are initiated by the NFC device and controlled by the Digital Control Unit of the NTAG21x. The command response is depending on the state of the IC and for memory operations also on the access conditions valid for the corresponding page.



Remark: In all states, the command interpreter returns to the idle state on receipt of an unexpected command. If the IC was previously in the HALT state, it returns to that state.

Fig 4. State diagram

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

8.4.1 IDLE state

After a power-on reset (POR), NTAG21x switches to the IDLE state. It only exits this state when a REQA or a WUPA command is received from the NFC device. Any other data received while in this state is interpreted as an error and NTAG21x remains in the IDLE state.

After a correctly executed HLTA command i.e. out of the ACTIVE or AUTHENTICATED state, the default waiting state changes from the IDLE state to the HALT state. This state can then be exited with a WUPA command only.

8.4.2 READY1 state

In this state, the NFC device resolves the first part of the UID (3 bytes) using the ANTICOLLISION or SELECT commands in cascade level 1. This state is correctly exited after execution of either of the following commands:

- SELECT command from cascade level 1: the NFC device switches NTAG21x into READY2 state where the second part of the UID is resolved.
- READ command (from address 0): all anticollision mechanisms are bypassed and the NTAG21x switches directly to the ACTIVE state.

Remark: If more than one NTAG is in the NFC device field, a READ command from address 0 selects all NTAG21x devices. In this case, a collision occurs due to different serial numbers. Any other data received in the READY1 state is interpreted as an error and depending on its previous state NTAG21x returns to the IDLE or HALT state.

8.4.3 READY2 state

In this state, NTAG21x supports the NFC device in resolving the second part of its UID (4 bytes) with the cascade level 2 ANTICOLLISION command. This state is usually exited using the cascade level 2 SELECT command.

Alternatively, READY2 state can be skipped using a READ command (from address 0) as described for the READY1 state.

Remark: The response of NTAG21x to the cascade level 2 SELECT command is the Select AcKnowledge (SAK) byte. In accordance with ISO/IEC 14443, this byte indicates if the anticollision cascade procedure has finished. NTAG21x is now uniquely selected and only this device will communicate with the NFC device even when other contactless devices are present in the NFC device field. If more than one NTAG21x is in the NFC device field, a READ command from address 0 selects all NTAG21x devices. In this case, a collision occurs due to the different serial numbers. Any other data received when the device is in this state is interpreted as an error. Depending on its previous state the NTAG21x returns to either the IDLE state or HALT state.

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

8.4.4 ACTIVE state

All memory operations and other functions like the originality signature read-out are operated in the ACTIVE state.

The ACTIVE state is exited with the HLTA command and upon reception NTAG21x transits to the HALT state. Any other data received when the device is in this state is interpreted as an error. Depending on its previous state NTAG21x returns to either the IDLE state or HALT state.

NTAG21x transits to the AUTHENTICATED state after successful password verification using the PWD_AUTH command.

8.4.5 AUTHENTICATED state

In this state, all operations on memory pages, which are configured as password verification protected, can be accessed.

The AUTHENTICATED state is exited with the HLTA command and upon reception NTAG21x transits to the HALT state. Any other data received when the device is in this state is interpreted as an error. Depending on its previous state NTAG21x returns to either the IDLE state or HALT state.

8.4.6 HALT state

HALT and IDLE states constitute the two wait states implemented in NTAG21x. An already processed NTAG21x can be set into the HALT state using the HLTA command. In the anticollision phase, this state helps the NFC device to distinguish between processed tags and tags yet to be selected. NTAG21x can only exit this state on execution of the WUPA command. Any other data received when the device is in this state is interpreted as an error and NTAG21x state remains unchanged.

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

8.5 Memory organization

The EEPROM memory is organized in pages with 4 bytes per page. NTAG213 variant has 45 pages, NTAG215 variant has 135 pages and NTAG216 variant has 231 pages in total. The memory organization can be seen in Figure 5, Figure 6 and Figure 7, the functionality of the different memory sections is described in the following sections.

Page Adr		Byte number within a page				Description
Dec	Hex	0	1	2	3	
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

Fig 5. Memory organization NTAG213

The structure of manufacturing data, lock bytes, capability container and user memory pages are compatible to NTAG203.

Page Adr		Byte number within a page				Description
Dec	Hex	0	1	2	3	
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					
...	...					
128	80h					
129	81h					
130	82h	dynamic lock bytes			RFUI	Dynamic lock bytes
131	83h	CFG 0				Configuration pages
132	84h	CFG 1				
133	85h	PWD				
134	86h	PACK		RFUI		

aaa-008088

Fig 6. Memory organization NTAG215

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

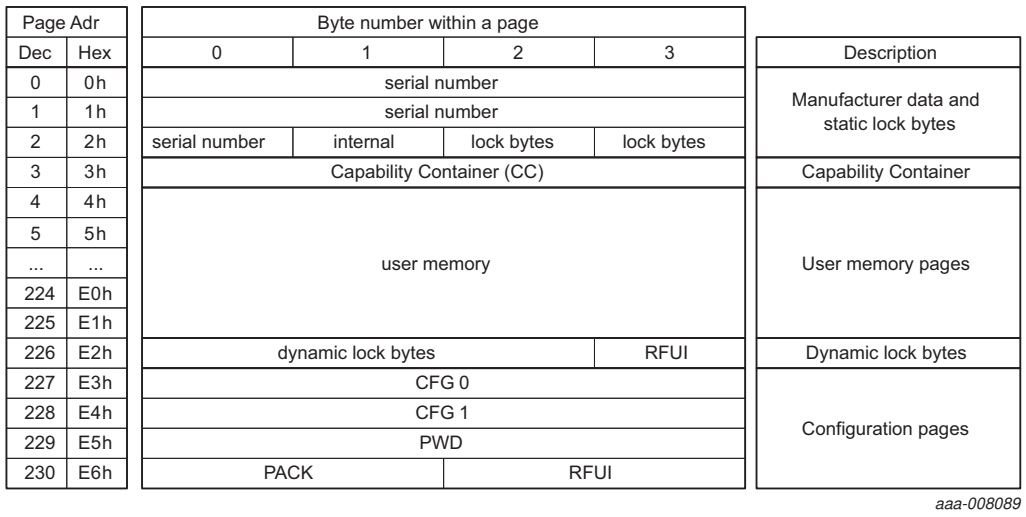


Fig 7. Memory organization NTAG216

8.5.1 UID/serial number

The unique 7-byte serial number (UID) and its two check bytes are programmed into the first 9 bytes of memory covering page addresses 00h, 01h and the first byte of page 02h. The second byte of page address 02h is reserved for internal data. These bytes are programmed and write protected in the production test.

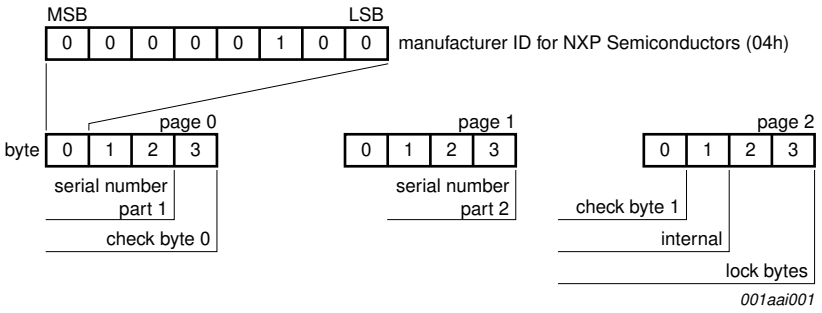


Fig 8. UID/serial number

In accordance with ISO/IEC 14443-3 check byte 0 (BCC0) is defined as CT Å SN0 Å SN1 Å SN2 and check byte 1 (BCC1) is defined as SN3 Å SN4 Å SN5 Å SN6.

SN0 holds the Manufacturer ID for NXP Semiconductors (04h) in accordance with ISO/IEC 14443-3.

8.5.2 Static lock bytes (NTAG21x)

The bits of byte 2 and byte 3 of page 02h 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.

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

The three least significant bits of lock byte 0 are the block-locking bits. Bit 2 deals with pages 0Ah to 0Fh, bit 1 deals with pages 04h to 09h and bit 0 deals with page 03h (CC). Once the block-locking bits are set, the locking configuration for the corresponding memory area is frozen.

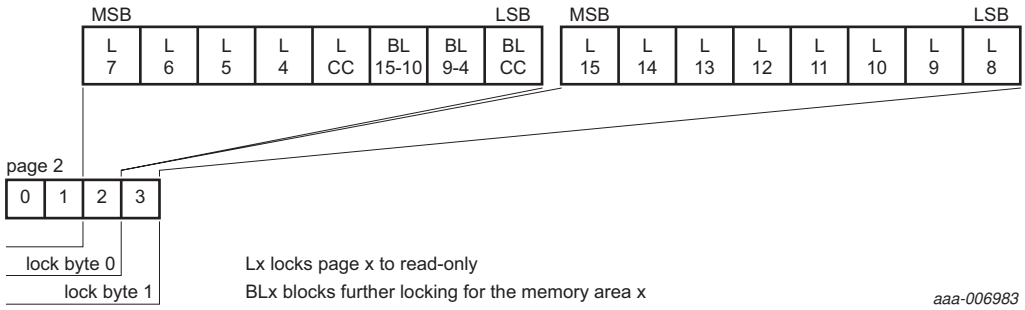


Fig 9. Static lock bytes 0 and 1

For example if BL15-10 is set to logic 1, then bits L15 to L10 (lock byte 1, bit[7:2]) can no longer be changed. The so called static locking and block-locking bits are set by a WRITE or COMPATIBILITY_WRITE command to page 02h. Bytes 2 and 3 of the WRITE or COMPATIBILITY_WRITE command, and the contents of the lock bytes are bit-wise OR'ed and the result then becomes the new content of the lock bytes. This process is irreversible. If a bit is set to logic 1, it cannot be changed back to logic 0.

The contents of bytes 0 and 1 of page 02h are unaffected by the corresponding data bytes of the WRITE or COMPATIBILITY_WRITE command.

The default value of the static lock bytes is 00 00h.

Any write operation to the static lock bytes is tearing-proof.

8.5.3 Dynamic Lock Bytes

To lock the pages of NTAG21x starting at page address 10h and onwards, the so called dynamic lock bytes are used. The dynamic lock bytes are located at page 28h for NTAG213, at page 82h for NTAG215 and at page E2h for NTAG216. The three lock bytes cover the memory area of 96 data bytes for NTAG213, 456 data bytes for NTAG215 and 840 data bytes for NTAG216. The granularity is 2 pages for NTAG213 (Figure 10) and 16 pages for NTAG215 (Figure 11) and NTAG216 (Figure 12).

Remark: Set all bits marked with RFUI to 0, when writing to the dynamic lock bytes.

Remark: For the correct usage of the dynamic lock bytes with NFC devices for the NTAG215 and NTAG216 refer to Ref. 9 "AN11456 NTAG215/216(F)/NTAG I2C Using the dynamic lock bits to lock the tag".

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

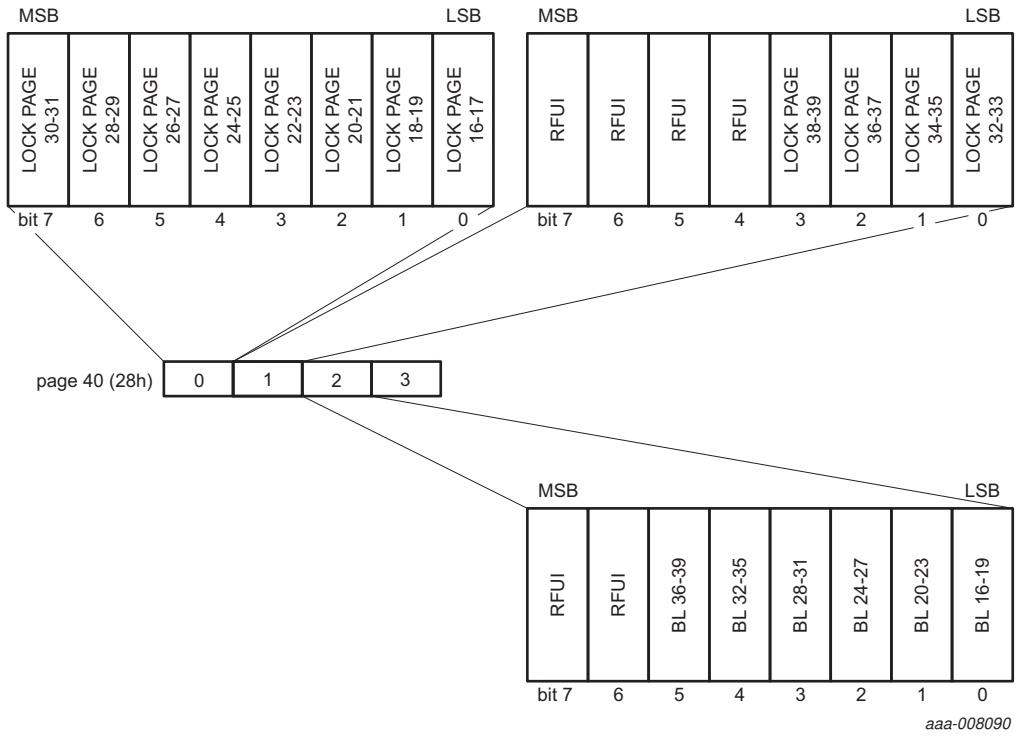


Fig 10. NTAG213 Dynamic lock bytes 0, 1 and 2

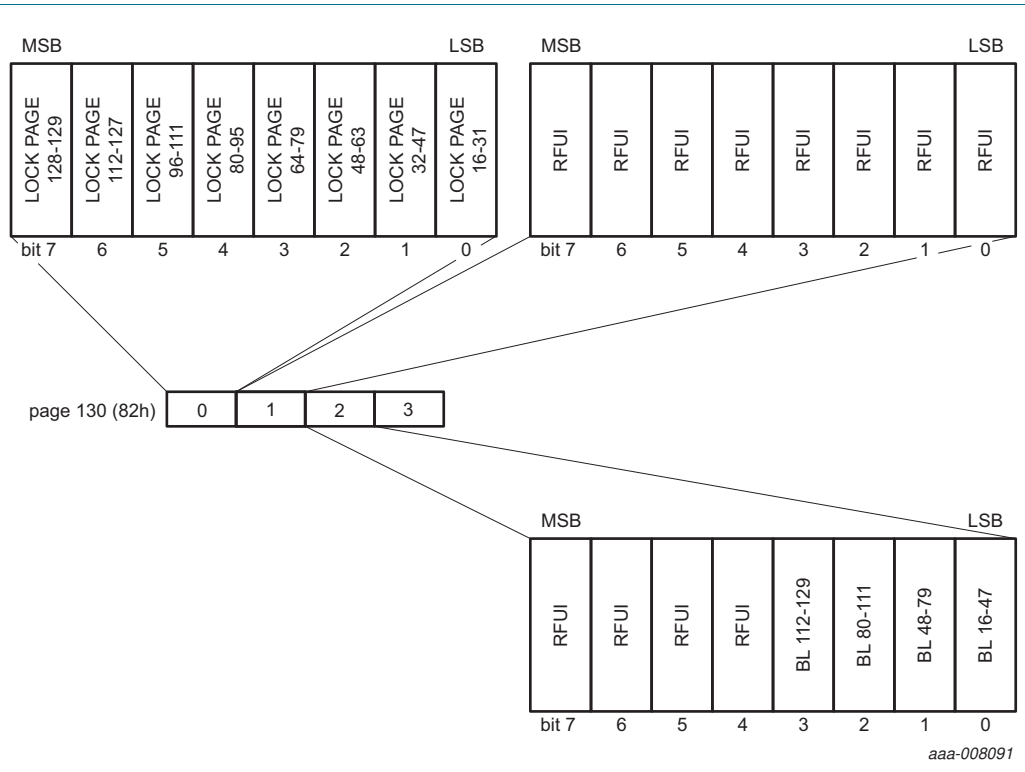


Fig 11. NTAG215 Dynamic lock bytes 0, 1 and 2

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

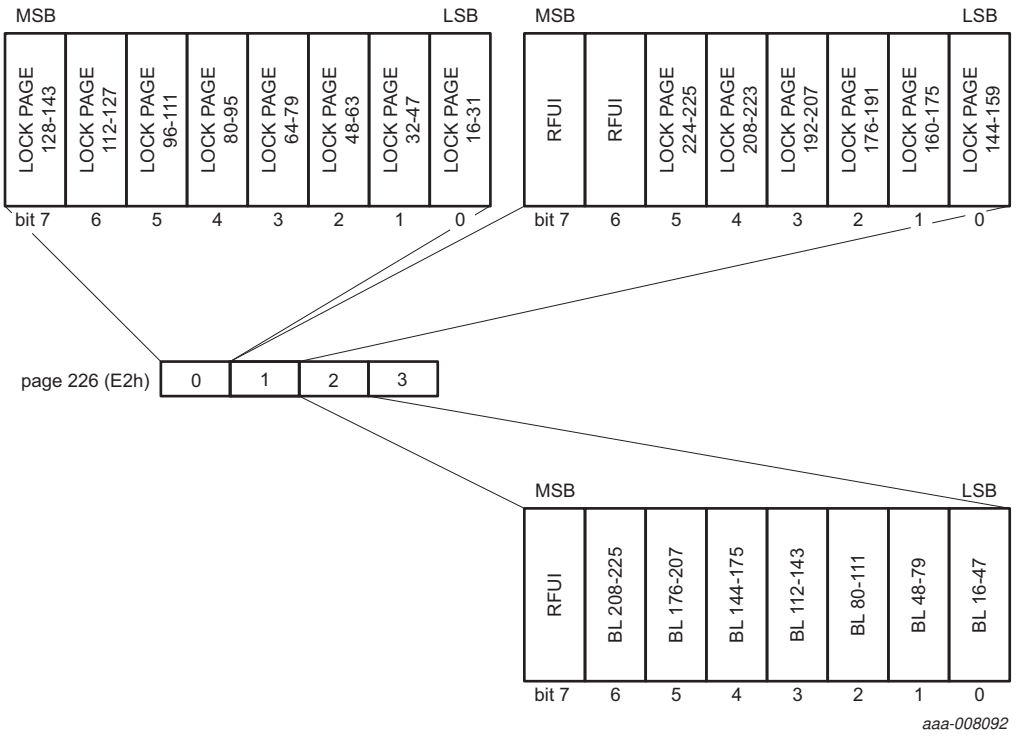


Fig 12. NTAG216 Dynamic lock bytes 0, 1 and 2

The default value of the dynamic lock bytes is 00 00 00h. The value of Byte 3 is always BDh when read.

Any write operation to the dynamic lock bytes is tearing-proof.

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

8.5.4 Capability Container (CC bytes)

The Capability Container CC (page 3) is programmed during the IC production according to the NFC Forum Type 2 Tag specification (see Ref. 2). These bytes may be bit-wise modified by a WRITE or COMPATIBILITY_WRITE command.

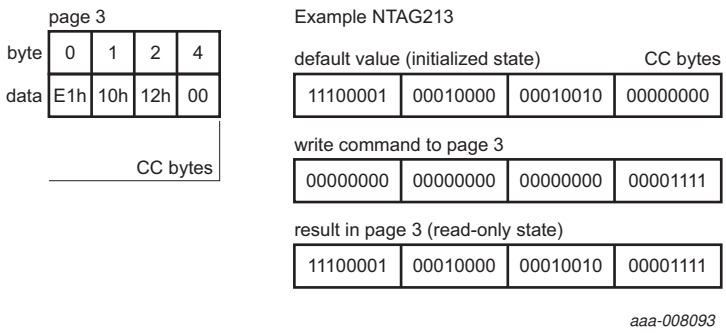


Fig 13. CC bytes example

The parameter bytes of the WRITE command and the current contents of the CC bytes are bit-wise OR'ed. The result is the new CC byte contents. This process is irreversible and once a bit is set to logic 1, it cannot be changed back to logic 0.

Byte 2 in the capability container defines the available memory size for NDEF messages. The configuration at delivery is shown in Table 4.

Table 4. NDEF memory size

IC	Value in byte 2	NDEF memory size
NTAG213	12h	144 byte
NTAG215	3Eh	496 byte
NTAG216	6Dh	872 byte

Any write operation to the CC bytes is tearing-proof.

The default values of the CC bytes at delivery are defined in Section 8.5.6.

8.5.5 Data pages

Pages 04h to 27h for NTAG213, pages 04h to 81h for NTAG215 and pages 04h to E1h for NTAG216 are the user memory read/write area.

The access to a part of the user memory area can be restricted using a password verification. See Section 8.8 for further details.

The default values of the data pages at delivery are defined in Section 8.5.6.

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

8.5.6 Memory content at delivery

The capability container in page 03h and the data pages 04h and 05h of NTAG21x are pre-programmed as defined in Table 5, Table 6 and Table 7.

Table 5. Memory content at delivery NTAG213

Page Address	Byte number within page			
	0	1	2	3
03h	E1h	10h	12h	00h
04h	01h	03h	A0h	0Ch
05h	34h	03h	00h	FEh

Table 6. Memory content at delivery NTAG215

Page Address	Byte number within page			
	0	1	2	3
03h	E1h	10h	3Eh	00h
04h	03h	00h	FEh	00h
05h	00h	00h	00h	00h

Table 7. Memory content at delivery NTAG216

Page Address	Byte number within page			
	0	1	2	3
03h	E1h	10h	6Dh	00h
04h	03h	00h	FEh	00h
05h	00h	00h	00h	00h

The access to a part of the user memory area can be restricted using a password verification. Please see Section 8.8 for further details.

Remark: The default content of the data pages from page 05h onwards is not defined at delivery.

Remark: For the correct usage of the dynamic lock bytes with NFC devices for the NTAG215 and NTAG216 refer to Ref. 9 “AN11456 NTAG215/216(F)/NTAG I2C Using the dynamic lock bits to lock the tag”.

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

8.5.7 Configuration pages

Pages 29h to 2Ch for NTAG213, pages 83h to 86h for NTAG215 and pages E3h to E6h for NTAG216 are used to configure the memory access restriction and to configure the UID ASCII mirror feature. The memory content of the configuration pages is detailed below.

Table 8. Configuration Pages

Page Address[1]		Byte number			
Dec	Hex	0	1	2	3
41/131/227	29h/83h/E3h	MIRROR	RFUI	MIRROR_PAGE	AUTH0
42/132/228	2Ah/84h/E4h	ACCESS	RFUI	RFUI	RFUI
43/133/229	2Bh/85h/E5h	PWD			
44/134/230	2Ch/86h/E6h	PACK		RFUI	RFUI

[1] Page address for resp. NTAG213/NTAG215/NTAG216

Table 9. MIRROR configuration byte

Bit number							
7	6	5	4	3	2	1	0
MIRROR_CONF		MIRROR_BYTE		RFUI	STRG_MOD_EN	RFUI	

Table 10. ACCESS configuration byte

Bit number							
7	6	5	4	3	2	1	0
PROT	CFGLCK	RFUI	NFC_CNT_EN	NFC_CNT_PWD_PROT	AUTHLIM		

Table 11. Configuration parameter descriptions

Field	Bit	Default values	Description
MIRROR_CONF	2	00b	Defines which ASCII mirror shall be used, if the ASCII mirror is enabled by a valid the MIRROR_PAGE byte 00b ... no ASCII mirror 01b ... UID ASCII mirror 10b ... NFC counter ASCII mirror 11b ... UID and NFC counter ASCII mirror
MIRROR_BYTE	2	00b	The 2 bits define the byte position within the page defined by the MIRROR_PAGE byte (beginning of ASCII mirror)
STRG_MOD_EN	1	1b	STRG MOD_EN defines the modulation mode 0b ... strong modulation mode disabled 1b ... strong modulation mode enabled

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

Table 11. Configuration parameter descriptions

Field	Bit	Default values	Description
MIRROR_PAGE	8	00h	MIRROR_Page defines the page for the beginning of the ASCII mirroring A value >03h enables the ASCII mirror feature
AUTH0	8	FFh	AUTH0 defines the page address from which the password verification is required. Valid address range for byte AUTH0 is from 00h to FFh. If AUTH0 is set to a page address which is higher than the last page from the user configuration, the password protection is effectively disabled.
PROT	1	0b	One bit inside the ACCESS byte defining the memory protection 0b ... write access is protected by the password verification 1b ... read and write access is protected by the password verification
CFGLCK	1	0b	Write locking bit for the user configuration 0b ... user configuration open to write access 1b ... user configuration permanently locked against write access, except PWD and PACK
NFC_CNT_EN	1	0b	NFC counter configuration 0b ... NFC counter disabled 1b ... NFC counter enabled If the NFC counter is enabled, the NFC counter will be automatically increased at the first READ or FAST_READ command after a power on reset
NFC_CNT_PWD_PROT	1	0b	NFC counter password protection 0b ... NFC counter not protected 1b ... NFC counter password protection enabled If the NFC counter password protection is enabled, the NFC tag will only respond to a READ_CNT command with the NFC counter value after a valid password verification
AUTHLIM	3	000b	Limitation of negative password verification attempts 000b ... limiting of negative password verification attempts disabled 001b-111b ... maximum number of negative password verification attempts
PWD	32	FFFFFFFFh	32-bit password used for memory access protection
PACK	16	0000h	16-bit password acknowledge used during the password verification process
RFUI	-	all 0b	Reserved for future use - implemented. Write all bits and bytes denoted as RFUI as 0b.

Remark: The CFGLCK bit activates the permanent write protection of the first two configuration pages. The write lock is only activated after a power cycle of NTAG21x. If write protection is enabled, each write attempt leads to a NAK response.

8.6 NFC counter function

NTAG21x features a NFC counter function. This function enables NTAG21x to automatically increase the 24 bit counter value, triggered by the first valid

- READ command or
- FAST-READ command

after the NTAG21x tag is powered by an RF field.

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

Once the NFC counter has reached the maximum value of FF FF FF hex, the NFC counter value will not change any more.

The NFC counter is enabled or disabled with the NFC_CNT_EN bit (see Section 8.5.7).

The actual NFC counter value can be read with

- READ_CNT command or
- NFC counter mirror feature

The reading of the NFC counter (by READ_CNT command or with the NFC counter mirror) can also be protected with the password authentication. The NFC counter password protection is enabled or disabled with the NFC_CNT_PWD_PROT bit (see Section 8.5.7).

8.7 ASCII mirror function

NTAG21x features a ASCII mirror function. This function enables NTAG21x to virtually mirror

- 7 byte UID (see Section 8.7.1) or
- 3 byte NFC counter value (see Section 8.7.2) or
- both, 7 byte UID and 3 byte NFC counter value with a separation byte (see Section 8.7.3)

into the physical memory of the IC in ASCII code. On the READ or FAST READ command to the involved user memory pages, NTAG21x will respond with the virtual memory content of the UID and/or NFC counter value in ASCII code.

The required length of the reserved physical memory for the mirror functions is specified in Table 12. If the ASCII mirror exceeds the user memory area, the data will not be mirrored.

Table 12. Required memory space for ASCII mirror

ASCII mirror	Required number of bytes in the physical memory
UID mirror	14 bytes
NFC counter	6 bytes
UID + NFC counter mirror	21 bytes (14 bytes for UID + 1 byte separation + 6 bytes NFC counter value)

The position within the user memory where the mirroring of the UID and/or NFC counter shall start is defined by the MIRROR_PAGE and MIRROR_BYTE values.

The MIRROR_PAGE value defines the page where the ASCII mirror shall start and the MIRROR_BYTE value defines the starting byte within the defined page.

The ASCII mirror function is enabled with a MIRROR_PAGE value >03h.

The MIRROR_CONF bits (see Table 9 and Table 11) define if ASCII mirror shall be enabled for the UID and/or NFC counter.

If both, the UID and NFC counter, are enabled for the ASCII mirror, the UID and the NFC counter bytes are separated automatically with an “x” character (78h ASCII code).

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

8.7.1 UID ASCII mirror function

This function enables NTAG21x to virtually mirror the 7 byte UID in ASCII code into the physical memory of the IC. The length of the UID ASCII mirror requires 14 bytes to mirror the UID in ASCII code. On the READ or FAST READ command to the involved user memory pages, NTAG21x will respond with the virtual memory content of the UID in ASCII code.

The position within the user memory where the mirroring of the UID shall start is defined by the MIRROR_PAGE and MIRROR_BYTE values.

The MIRROR_PAGE value defines the page where the UID ASCII mirror shall start and the MIRROR_BYTE value defines the starting byte within the defined page.

The UID ASCII mirror function is enabled with a MIRROR_PAGE value >03h and the MIRROR_CONF bits are set to 01b.

Remark: Please note that the 14 bytes of the UID ASCII mirror shall not exceed the boundary of the user memory. Therefore it is required to use only valid values for MIRROR_BYTE and MIRROR_PAGE to ensure a proper functionality. If the UID ASCII mirror exceeds the user memory area, the UID will not be mirrored.

Table 13. Configuration parameter description

	MIRROR_PAGE	MIRROR_BYTE bits
Minimum values	04h	00b
Maximum values	last user memory page - 3	01b

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

8.7.1.1 UID ASCII Mirror example

Table 14 show the memory content of a NTAG213 which has been written to the physical memory. Without the UID ASCII mirror feature, the content in the user memory would be a URL according to the NFC Data Exchange Format (NDEF) Ref. 3 with the content:

http://www.nxp.com/index.html?m=00000000000000

Table 14. UID ASCII mirror - Physical memory content

Page address		Byte number				
dec.	**hex.**	**0**	**1**	**2**	**3**	**ASCII**
0	00h	04	E1	41	2C	
1	01h	12	4C	28	80	
2	02h	F6	internal	lock bytes		
3	03h	E1	10	12	00	
4	04h	01	03	A0	0C	....
5	05h	34	03	28	D1	4.(.
6	06h	01	24	55	01	.$U.
7	07h	6E	78	70	2E	nxp.
8	08h	63	6F	6D	2F	com/
9	09h	69	6E	64	65	inde
10	0Ah	78	2E	68	74	x.ht
11	0Bh	6D	6C	3F	6D	ml?m
12	0Ch	3D	30	30	30	=000
13	0Dh	30	30	30	30	0000
14	0Eh	30	30	30	30	0000
15	0Fh	30	30	30	FE	000.
16	10h	00	00	00	00	....
...	...					
39	27h	00	00	00	00	....
40	28h	dynamic lock bytes			RFUI	
41	29h	54	RFUI	0C	AUTH0	
42	2Ah	Access				
43	2Bh	PWD				
44	2Ch	PACK		RFUI		

With the UID Mirror feature and the related values in the MIRROR_PAGE and the MIRROR_BYTE the UID 04-E1-41-12-4C-28-80h will be mirrored in ASCII code into the user memory starting in page 0Ch byte 1. The virtual memory content is shown in Table 15.

Reading the user memory, the data will be returned as an URL according to the NFC Data Exchange Format (NDEF) Ref. 3 with the content:

http://www.nxp.com/index.html?m=04E141124C2880

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

Table 15. UID ASCII mirror - Virtual memory content

Page address		Byte number				
dec.	**hex.**	**0**	**1**	**2**	**3**	**ASCII**
0	00h	04	E1	41	2C	
1	01h	12	4C	28	80	
2	02h	F6	internal	lock bytes		
3	03h	E1	10	12	00	
4	04h	01	03	A0	0C	....
5	05h	34	03	28	D1	4.(.
6	06h	01	24	55	01	.$U.
7	07h	6E	78	70	2E	nxp.
8	08h	63	6F	6D	2F	com/
9	09h	69	6E	64	65	inde
10	0Ah	78	2E	68	74	x.ht
11	0Bh	6D	6C	3F	6D	ml?m
12	0Ch	3D	30	34	45	=04E
13	0Dh	31	34	31	31	1411
14	0Eh	32	34	43	32	24C2
15	0Fh	38	38	30	FE	880.
16	10h	00	00	00	00	....
...	...					
39	27h	00	00	00	00	....
40	28h	dynamic lock bytes			RFUI	
41	29h	54	RFUI	0C	AUTH0	
42	2Ah	Access				
43	2Bh	PWD				
44	2Ch	PACK		RFUI		

8.7.2 NFC counter mirror function

This function enables NTAG21x to virtually mirror the 3 byte NFC counter value in ASCII code into the physical memory of the IC. The length of the NFC counter mirror requires 6 bytes to mirror the NFC counter value in ASCII code. On the READ or FAST READ command to the involved user memory pages, NTAG21x will respond with the virtual memory content of the NFC counter in ASCII code.

The position within the user memory where the mirroring of the NFC counter shall start is defined by the MIRROR_PAGE and MIRROR_BYTE values.

The MIRROR_PAGE value defines the page where the NFC counter mirror shall start and the MIRROR_BYTE value defines the starting byte within the defined page.

The NFC counter mirror function is enabled with a MIRROR_PAGE value >03h and the MIRROR_CONF bits are set to 10b.

If the NFC counter is password protected with the NFC_CNT_PWD_PROT bit set to 1b (see Section 8.5.7), the NFC counter will only be mirrored into the physical memory, if a valid password authentication has been executed before.

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

Remark: To enable the NFC counter itself (see Section 8.6), the NFC_CNT_EN bit shall be set to 1b.

Remark: Please note that the 6 bytes of the NFC counter mirror shall not exceed the boundary of the user memory. Therefore it is required to use only valid values for MIRROR_BYTE and MIRROR_PAGE to ensure a proper functionality. If the NFC counter mirror exceeds the user memory area, the NFC counter will not be mirrored.

Table 16. Configuration parameter description

	MIRROR_PAGE	MIRROR_BYTE bits
Minimum values	04h	00b
Maximum values	last user memory page - 1	01b

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.

8.7.2.1 NFC counter mirror example

Table 17 show the memory content of a NTAG213 which has been written to the physical memory. Without the NFC counter mirror feature, the content in the user memory would be a URL according to the NFC Data Exchange Format (NDEF) Ref. 3 with the content:

http://www.nxp.com/index.html?m=000000

Table 17. NFC counter mirror - Physical memory content

Page address		Byte number				
dec.	**hex.**	**0**	**1**	**2**	**3**	**ASCII**
0	00h	04	E1	41	2C	
1	01h	12	4C	28	80	
2	02h	F6	internal	lock bytes		
3	03h	E1	10	12	00	
4	04h	01	03	A0	0C	....
5	05h	34	03	20	D1	4.(.
6	06h	01	1C	55	01	.$U.
7	07h	6E	78	70	2E	nxp.
8	08h	63	6F	6D	2F	com/
9	09h	69	6E	64	65	inde
10	0Ah	78	2E	68	74	x.ht
11	0Bh	6D	6C	3F	6D	ml?m
12	0Ch	3D	30	30	30	=000
13	0Dh	30	30	30	FE	000.
14	0Eh	00	00	00	00	....
...	...					
39	27h	00	00	00	00	....
40	28h	dynamic lock bytes			RFUI	
41	29h	94	RFUI	0C	AUTH0	
42	2Ah	Access				
43	2Bh	PWD				
44	2Ch	PACK		RFUI		

With the NFC counter mirror feature and the related values in the MIRROR_PAGE and the MIRROR_BYTE the NFC counter value of e.g. 00-3F-31h will be mirrored in ASCII code into the user memory starting in page 0Ch byte 1. The virtual memory content is shown in Table 18.

Reading the user memory, the data will be returned as an URL according to the NFC Data Exchange Format (NDEF) Ref. 3 with the content:

http://www.nxp.com/index.html?m=003F31

All information provided in this document is subject to legal disclaimers.

© NXP Semiconductors N.V. 2015. All rights reserved.