NTAG210/212

NFC Forum Type 2 Tag compliant IC with 48/128 bytes user memory

Rev. 3.0 — 14 March 2013
242330

Product data sheet
COMPANY PUBLIC

1. General description

NTAG210 and NTAG212 have been developed by NXP Semiconductors as standard NFC tag ICs to be used in mass market applications such as retail, gaming and publishing, in combination with NFC devices or NFC compliant Proximity Coupling Devices. NTAG210 and NTAG212 (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.

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.

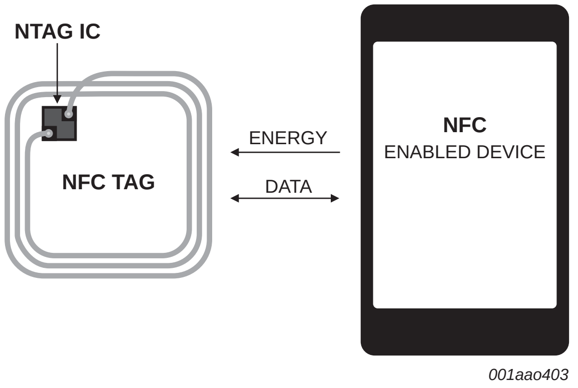


Fig 1. Contactless system

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
- Capability container with one time programmable bits
- Field programmable read-only locking function per page (per 2 pages for the extended memory section)
- 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.

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 NDEF messages
- ECC based originality signature
- Fast read command
- True anticollision

2.1 EEPROM

- 80 or 164 bytes organized in 20 or 41 pages with 4 bytes per page
- 48 or 128 bytes freely available user Read/Write area (12 or 32 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 per double page above the first 16 pages
- 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 simple pairing
- Connection handover

4. Quick reference data

Table 1. Quick reference data

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
C_i	input capacitance	[1]	-	17.0	-	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
NT2L1011G0DUF	FFC Bump	8 inch wafer, 75 μm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 48 bytes user memory, 17 pF input capacitance	-
NT2L1011G0DUD	FFC Bump	8 inch wafer, 120 μm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 48 bytes user memory, 17 pF input capacitance	-
NT2L1211G0DUF	FFC Bump	8 inch wafer, 75 μm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 128 bytes user memory, 17 pF input capacitance	-
NT2L1211G0DUD	FFC Bump	8 inch wafer, 120 μm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 128 bytes user memory, 17 pF input capacitance	-

6. Block diagram

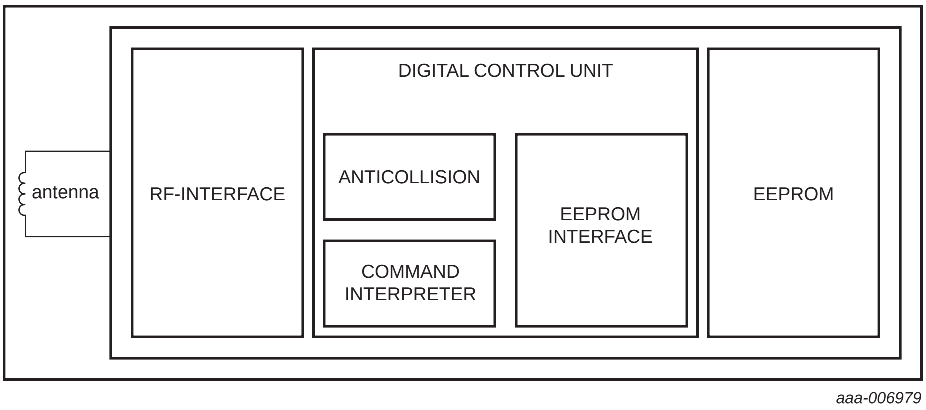


Fig 2. Block diagram of NTAG210/212

7. Pinning information

7.1 Pinning

The pinning of the NTAG210/212 wafer delivery is shown in section “Bare die outline” (see Section 13.2).

Table 3. Pin allocation table

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

8. Functional description

8.1 Block description

NTAG21x ICs consist of a 80 (NTAG210) or 164 bytes (NTAG212) 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
- NTAG210 EEPROM: 80 bytes, organized in 20 pages of 4 byte per page.
  - 26 bytes reserved for manufacturer and configuration data
  - 16 bits used for the read-only locking mechanism
  - 4 bytes available as capability container
  - 48 bytes user programmable read/write memory
- NTAG212 EEPROM: 164 bytes, organized in 41 pages of 4 byte per page.
  - 26 bytes reserved for manufacturer and configuration data
  - 31 bits used for the read-only locking mechanism
  - 4 bytes available as capability container
  - 128 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.

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.

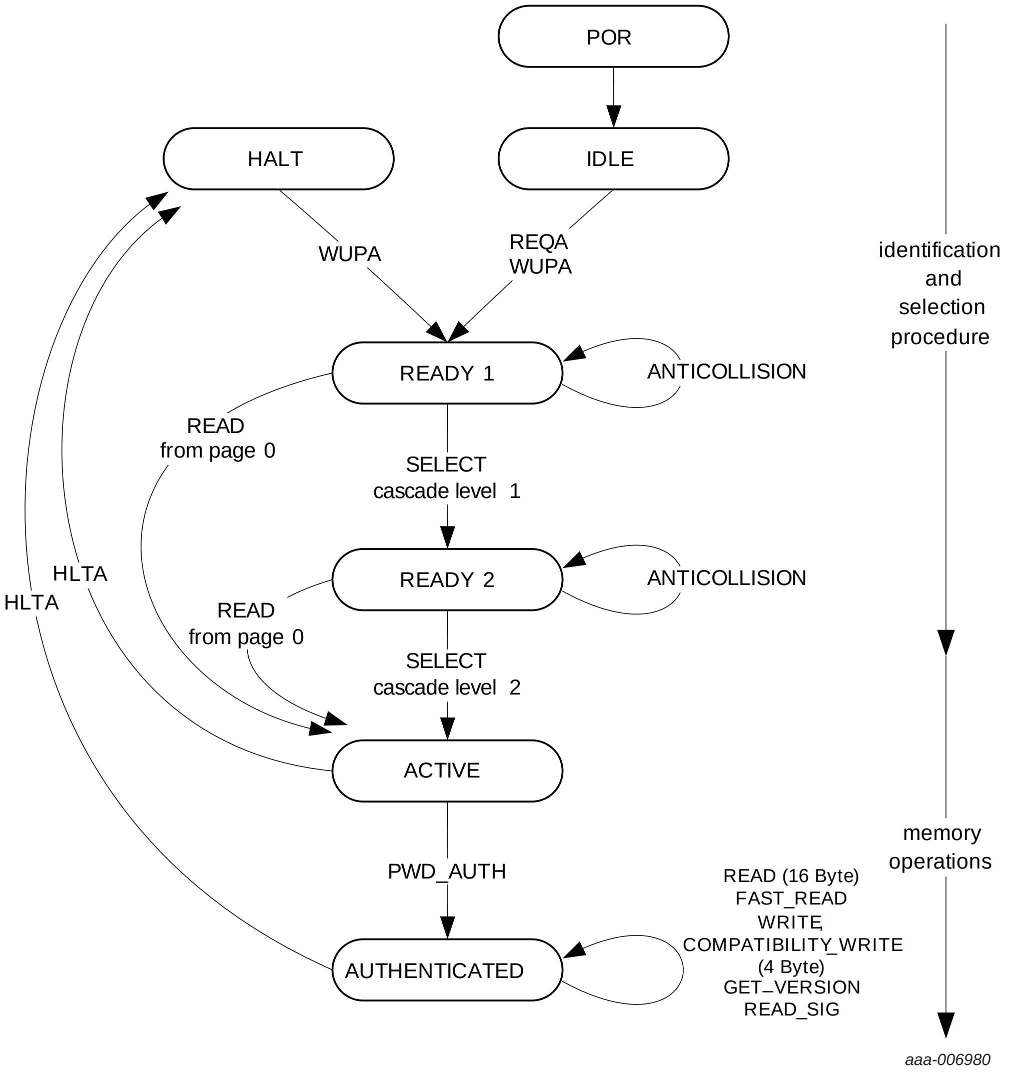
8.3 Data integrity

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)

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 3. State diagram

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.

8.4.4 ACTIVE state

All memory operations and other functions like the originality check 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.

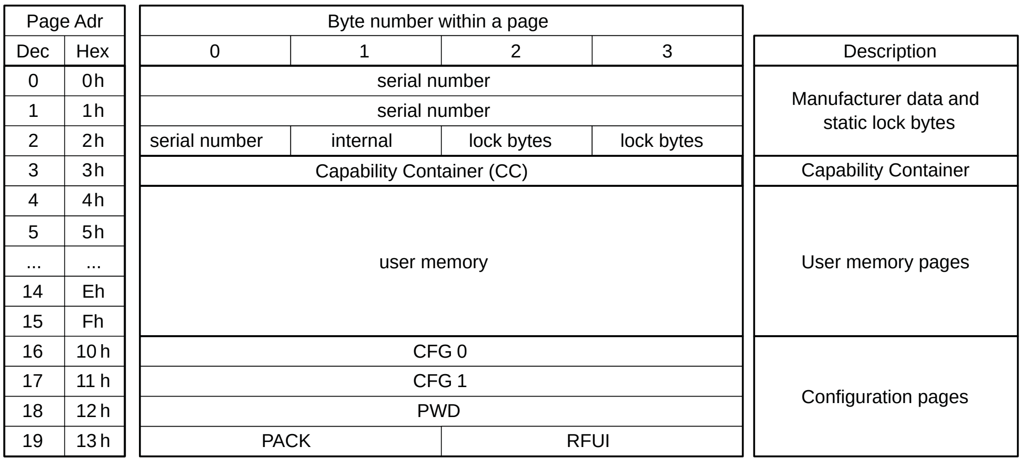
The AUTHENTICATED state is exited with the HLTA command and upon reception NTAG21x transits to the HALT state. Any other data received when the device is in this state is interpreted as an error. Depending on its previous state NTAG21x returns to either the IDLE state or HALT state.

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.

8.5 Memory organization

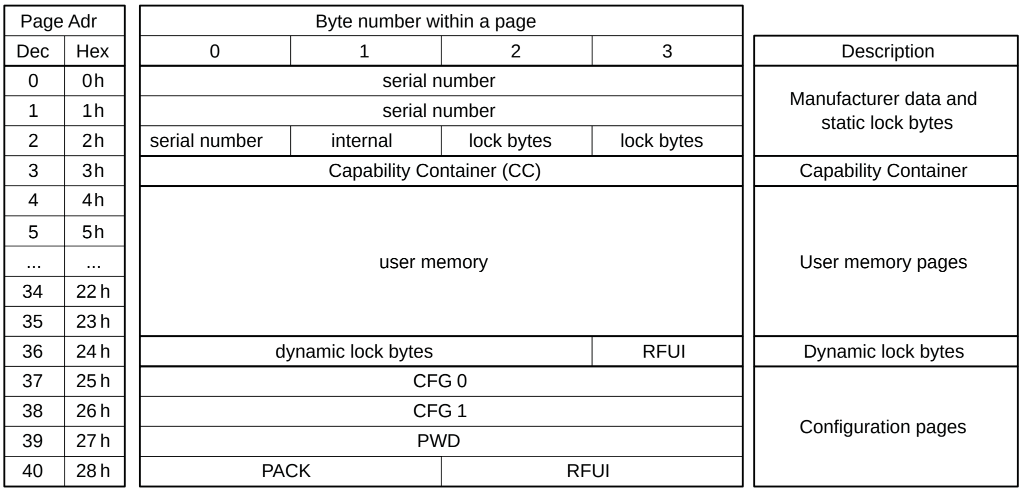
The EEPROM memory is organized in pages with 4 bytes per page. NTAG210 variant has 20 pages and NTAG212 variant has 41 pages in total. The memory organization can be seen in Figure 4 and Figure 5, the functionality of the different memory sections is described in the following sections.



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					
...	...					
14	Eh					
15	Fh					
16	10h	CFG 0				Configuration pages
17	11h	CFG 1				
18	12h	PWD				
19	13h	PACK		RFUI		

aaa-006981

Fig 4. Memory organization NTAG210



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					
...	...					
34	22h					
35	23h					
36	24h	dynamic lock bytes			RFUI	Dynamic lock bytes
37	25h	CFG 0				Configuration pages
38	26h	CFG 1				
39	27h	PWD				
40	28h	PACK		RFUI		

aaa-006982

Fig 5. Memory organization NTAG212

The structure of manufacturing data, static lock bytes, capability container and user memory pages (except of the user memory length) are compatible to NTAG203.

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.

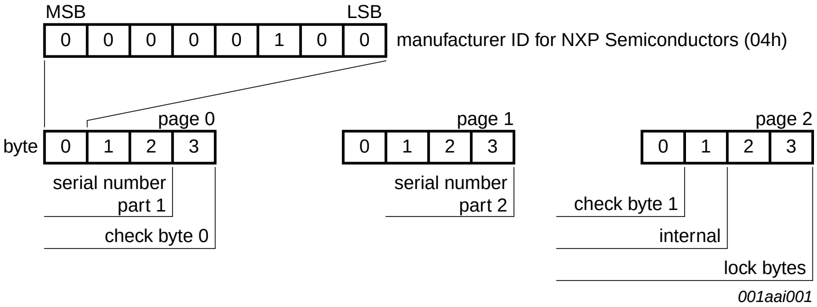


Fig 6. UID/serial number

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

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.

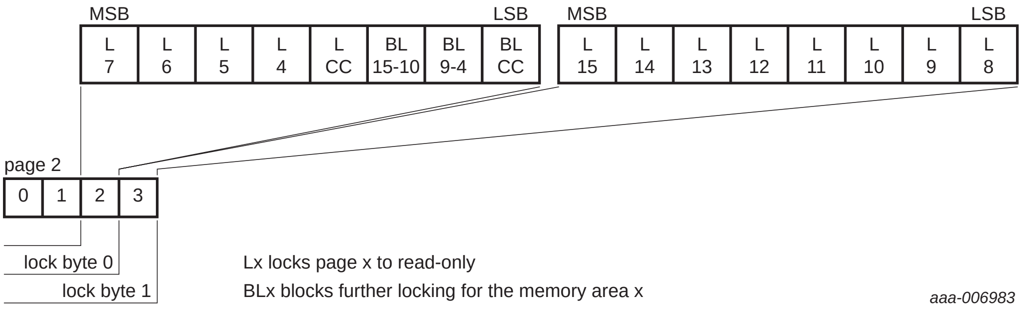


Fig 7. Static lock bytes 0 and 1

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 (NTAG212 only)

To lock the pages of NTAG212 starting at page address 10h and onwards, the so called dynamic lock bytes located in page 24h are used. Those three lock bytes cover the memory area of 80 data bytes.The granularity is 2 pages, compared to a single page for the first 64 bytes as shown in Figure 8.

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

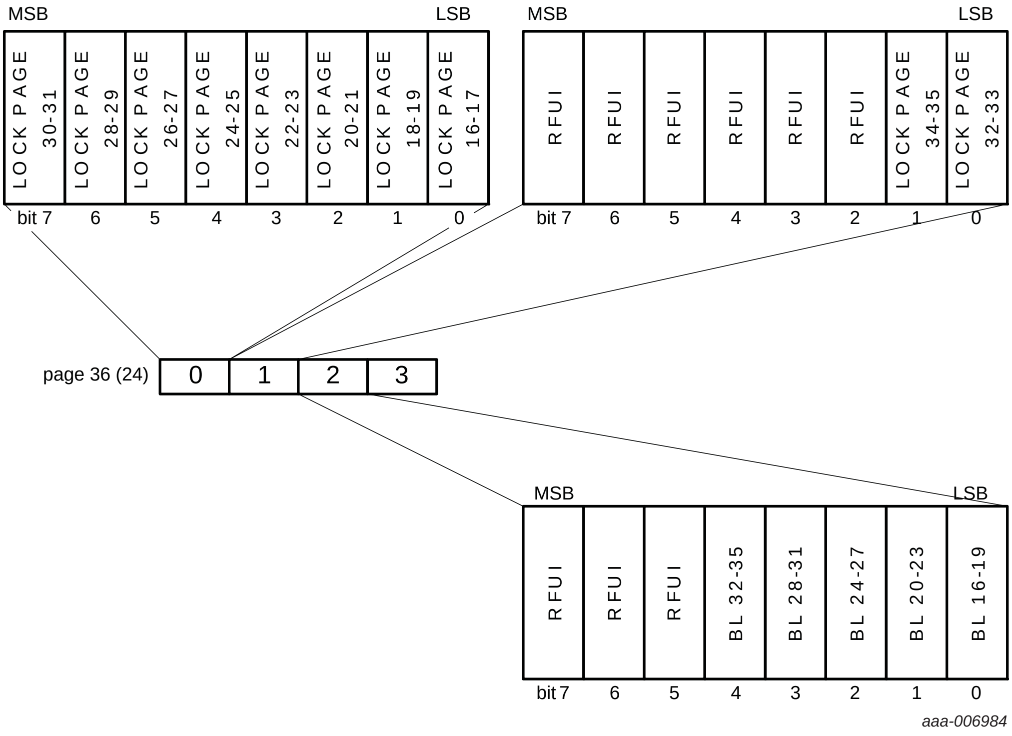


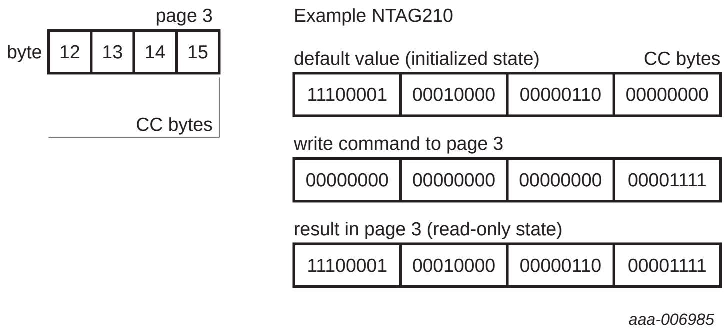
Fig 8. NTAG212 Dynamic lock bytes 0, 1 and 2

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.

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.



default value (initialized state)	11100001	00010000	00000110	00000000
write command to page 3	00000000	00000000	00000000	00001111
result in page 3 (read-only state)	11100001	00010000	00000110	00001111

This memory area can be used as a 32 tick one-time counter.

Fig 9. CC bytes

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.

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 0Fh for NTAG210 and 04h to 23h for NTAG212 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 8.7 for further details.

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

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 to the initialized state according to the NFC Forum Type 2 Tag specification (see Ref. 2) as defined in Table 4 and Table 5.

Table 4. Memory content at delivery NTAG210

Page Address	Byte number within page			
	0	1	2	3
03h	E1h	10h	06h	00h
04h	03h	00h	FEh	00h
05h	00h	00h	00h	00h

Table 5. Memory content at delivery NTAG212

Page Address	Byte number within page			
	0	1	2	3
03h	E1h	10h	10h	00h
04h	01h	03h	90h	0Ah
05h	34h	03h	00h	FEh

The access to a part of the user memory area can be restricted using a password verification. Please see Section 8.7 for further details.

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

8.5.7 Configuration pages

Pages 10h to 13h for NTAG210 and pages 25h to 28h for NTAG212 variant 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 6. Configuration Pages

Page Address[1]		Byte number			
Dec	**Hex**	**0**	**1**	**2**	**3**
16/37	10h/25h	MIRROR_BYTE	RFUI	MIRROR_PAGE	AUTH0
17/38	11h/26h	ACCESS	RFUI	RFUI	RFUI
18/39	12h/27h	PWD			
19/40	13h/28h	PACK		RFUI	RFUI

[1] Page address for resp. NTAG210 and NTAG212

Table 7. MIRROR_BYTE configuration byte

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

Table 8. ACCESS configuration byte

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

Table 9. Configuration parameter descriptions

Field	Bit	Default values	Description
MIRROR_BYTE	2	00b	The 2 bits define the byte position within the page defined by the MIRROR_PAGE byte (beginning of ASCII mirror)
MIRROR_PAGE	8	00h	MIRROR_Page defines the page for the beginning of the ASCII mirroring A value >03h enables the ASCII mirror feature 04h-0Ch ... valid MIRROR_PAGE values for NTAG210 04h-20h ... valid MIRROR_PAGE values for NTAG212
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
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

Table 9. Configuration parameter descriptions

Field	Bit	Default values	Description
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 UID ASCII mirror function

NTAG21x features a 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.

Remark: Please note that the 14 bytes of the UID ASCII mirror shall not exceed the boundary of the user memory. Therefor it is required to use only valid values for MIRROR_BYTE and MIRROR_PAGE to ensure a proper functionality.

Table 10. Configuration parameter descriptions

	MIRROR_PAGE	MIRROR_BYTE bits
Minimum values	04h	00b - 11b
Maximum value	last user memory page - 3	10b

8.6.1 UID ASCII Mirror example

Table 11 show the memory content of a NTAG210 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 11. 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	06	00	
4	04h	03	28	D1	01	.(..
5	05h	23	55	01	6E	#U.n
6	06h	78	70	2E	63	xp.c
7	07h	6F	6D	2F	69	om/i
8	08h	6E	64	65	78	ndex
9	09h	2E	68	74	6D	.htm
10	0Ah	6C	3F	6D	3D	l?m=
11	0Bh	**30**	**30**	**30**	**30**	**0000**
12	0Ch	**30**	**30**	**30**	**30**	**0000**
13	0Dh	**30**	**30**	**30**	**00**	**0000**
14	0Eh	**30**	**30**	FE	00	**00**..
15	0Fh	00	00	00	AUTH_DATA	....
16	10h	00	RFUI	0B		
17	11h	Access				
18	12h	PWD				
19	13h	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 0Bh byte 0. The virtual memory content is shown in Table 12.

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

Table 12. 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	06	00	
4	04h	03	28	D1	01	.(..
5	05h	23	55	01	6E	#U.n
6	06h	78	70	2E	63	xp.c
7	07h	6F	6D	2F	69	om/i
8	08h	6E	64	65	78	ndex
9	09h	2E	68	74	6D	.htm
10	0Ah	6C	3F	6D	3D	l?m=
11	0Bh	**30**	**34**	**45**	**31**	**04E1**
12	0Ch	**34**	**31**	**31**	**32**	**4112**
13	0Dh	**34**	**43**	**32**	**38**	**4C28**
14	0Eh	**38**	**30**	FE	00	**80**..
15	0Fh	00	00	00	AUTH_DATA	....
16	10h	00	RFUI	0B		
17	11h	Access				
18	12h	PWD				
19	13h	PACK		RFUI		

8.7 Password verification protection

The memory write or read/write access to a configurable part of the memory can be constrained to a positive password verification. The 32-bit secret password (PWD) and the 16-bit password acknowledge (PACK) response are typically programmed into the configuration pages at the tag personalization stage.

The AUTHLIM parameter specified in Section 8.5.7 can be used to limit the negative verification attempts.

In the initial state of NTAG21x, password protection is disabled by a AUTH0 value of FFh. PWD and PACK are freely writable in this state. Access to the configuration pages and any part of the user memory can be restricted by setting AUTH0 to a page address within the available memory space. This page address is the first one protected.

Remark: The password protection method provided in NTAG21x has to be intended as an easy and convenient way to prevent unauthorized memory accesses. If a higher level of protection is required, cryptographic methods can be implemented at application layer to increase overall system security.

8.7.1 Programming of PWD and PACK

The 32-bit PWD and the 16-bit PACK need to be programmed into the configuration pages, see Section 8.5.7. The password as well as the password acknowledge are written LSByte first. This byte order is the same as the byte order used during the PWD_AUTH command and its response.

The PWD and PACK bytes can never be read out of the memory. Instead of transmitting the real value on any valid READ or FAST_READ command, only 00h bytes are replied.

If the password verification does not protect the configuration pages, PWD and PACK can be written with normal WRITE and COMPATIBILITY_WRITE commands.

If the configuration pages are protected by the password configuration, PWD and PACK can be written after a successful PWD_AUTH command.

The PWD and PACK are writable even if the CFGLCK bit is set to 1b. Therefore it is strongly recommended to set AUTH0 to the page where the PWD is located after the password has been written. This page is 12h for NTAG210 and 27h for NTAG212.

Remark: To improve the overall system security, it is advisable to diversify the password and the password acknowledge using a die individual parameter of the iC, that is the 7-byte UID available on NTAG21x.

8.7.2 Limiting negative verification attempts

To prevent brute-force attacks on the password, the maximum allowed number of negative password verification attempts can be set using AUTHLIM. This mechanism is disabled by setting AUTHLIM to a value of 000b, which is also the initial state of NTAG21x.

If AUTHLIM is not equal to 000b, each negative authentication verification is internally counted. As soon as this internal counter reaches the number specified in AUTHLIM, any further negative password verification leads to a permanent locking of the protected part of the memory for the specified access modes. Specifically, whether the provided password is correct or not, each subsequent PWD_AUTH fails.

Any successful password verification, before reaching the limit of negative password verification attempts, resets the internal counter to zero.

8.7.3 Protection of special memory segments

The configuration pages can be protected by the password authentication as well. The protection level is defined with the PROT bit.

The protection is enabled by setting the AUTH0 byte to a value that is within the addressable memory space.

8.8 Originality signature

NTAG21x features a cryptographically supported originality check. With this feature, it is possible to verify with a certain confidence that the tag is using an IC manufactured by NXP Semiconductors. This check can be performed on personalized tags as well.

NTAG21x digital signature is based on standard Elliptic Curve Cryptography (curve name *secp128r1*), according to the ECDSA algorithm. The use of a standard algorithm and curve ensures easy software integration of the originality check procedure in NFC devices without specific hardware requirements.

Each NTAG21x UID is signed with a NXP private key and the resulting 32-byte signature is stored in a hidden part of the NTAG21x memory during IC production.

This signature can be retrieved using the READ_SIG command and can be verified in the NFC device by using the corresponding ECC public key provided by NXP. In case the NXP public key is stored in the NFC device, the complete signature verification procedure can be performed offline.

To verify the signature (for example with the use of the public domain crypto library *OpenSSL)* the tool domain parameters shall be set to *secp128r1,* defined within the standards for elliptic curve cryptography SEC (Ref. 7).

Details on how to check the signature value are provided in following application note (Ref. 5). It is foreseen to offer an online and offline way to verify originality of NTAG21x.

9. Command overview

NTAG activation follows the ISO/IEC 14443 Type A. After NTAG21x has been selected, it can either be deactivated using the ISO/IEC 14443 HLTA command, or the NTAG commands (e.g. READ or WRITE) can be performed. For more details about the card activation refer to Ref. 1.

9.1 NTAG21x command overview

All available commands for NTAG21x are shown in Table 13.

Table 13. Command overview

Command[1]	ISO/IEC 14443	NFC FORUM	Command code (hexadecimal)
Request	REQA	SENS_REQ	26h (7 bit)
Wake-up	WUPA	ALL_REQ	52h (7 bit)
Anticollision CL1	Anticollision CL1	SDD_REQ CL1	93h 20h
Select CL1	Select CL1	SEL_REQ CL1	93h 70h
Anticollision CL2	Anticollision CL2	SDD_REQ CL2	95h 20h
Select CL2	Select CL2	SEL_REQ CL2	95h 70h
Halt	HLTA	SLP_REQ	50h 00h
GET_VERSION[2]	-	-	60h
READ	-	READ	30h
FAST_READ[2]	-	-	3Ah
WRITE	-	WRITE	A2h
COMP_WRITE	-	-	A0h
PWD_AUTH[2]	-	-	1Bh
READ_SIG[2]	-	-	3Ch

[1] Unless otherwise specified, all commands use the coding and framing as described in Ref. 1.

[2] This command is new in NTAG21x compared to NTAG203.

9.2 Timings

The command and response timings shown in this document are not to scale and values are rounded to 1 μs.

All given command and response times refer to the data frames including start of communication and end of communication. They do not include the encoding (like the Miller pulses). A NFC device data frame contains the start of communication (1 “start bit”) and the end of communication (one logic 0 + 1 bit length of unmodulated carrier). A NFC tag data frame contains the start of communication (1 “start bit”) and the end of communication (1 bit length of no subcarrier).

The minimum command response time is specified according to Ref. 1 as an integer n which specifies the NFC device to NFC tag frame delay time. The frame delay time from NFC tag to NFC device is at least 87 μs. The maximum command response time is specified as a time-out value. Depending on the command, the T_{ACK} value specified for command responses defines the NFC device to NFC tag frame delay time. It does it for either the 4-bit ACK value specified in Section 9.3 or for a data frame.

All timing can be measured according to ISO/IEC 14443-3 frame specification as shown for the Frame Delay Time in Figure 10. For more details refer to Ref. 1.

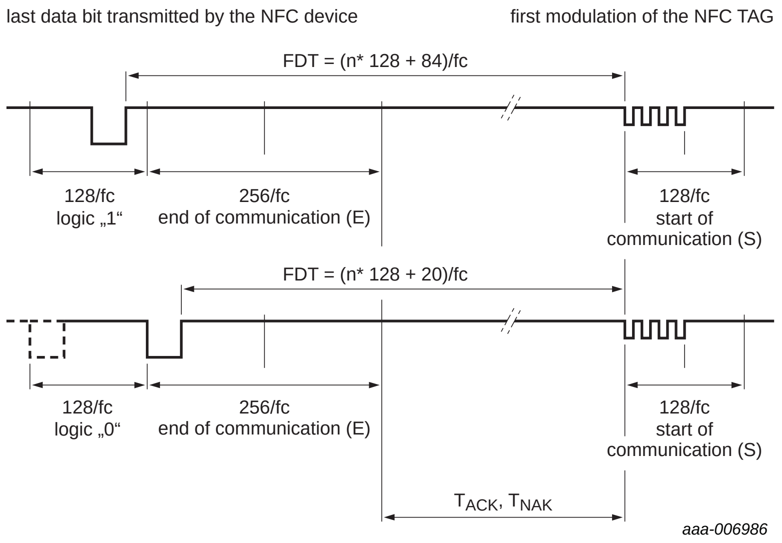


Fig 10. Frame Delay Time (from NFC device to NFC tag), T_{ACK} and T_{NAK}

Remark: Due to the coding of commands, the measured timings usually excludes (a part of) the end of communication. Considered this factor when comparing the specified with the measured times.

9.3 NTAG ACK and NAK

NTAG uses a 4 bit ACK / NAK as shown in Table 14.

Table 14. ACK and NAK values

Code (4-bit)	ACK/NAK
Ah	Acknowledge (ACK)
0h	NAK for invalid argument (i.e. invalid page address)
1h	NAK for parity or CRC error
5h	NAK for EEPROM write error

9.4 ATQA and SAK responses

NTAG21x replies to a REQA or WUPA command with the ATQA value shown in Table 15. It replies to a Select CL2 command with the SAK value shown in Table 16. The 2-byte ATQA value is transmitted with the least significant byte first (44h).

Table 15. ATQA response of the NTAG21x

		Bit number															
Sales type	**Hex value**	**16**	**15**	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
NTAG21x	00 44h	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0

Table 16. SAK response of the NTAG21x

		Bit number							
Sales type	**Hex value**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
NTAG21x	00h	0	0	0	0	0	0	0	0

Remark: The ATQA coding in bits 7 and 8 indicate the UID size according to ISO/IEC 14443 independent from the settings of the UID usage.

Remark: The bit numbering in the ISO/IEC 14443 starts with LSB = bit 1 and not with LSB = bit 0. So 1 byte counts bit 1 to bit 8 instead of bit 0 to 7.

10. NTAG commands

10.1 GET_VERSION

The GET_VERSION command is used to retrieve information on the NTAG family, the product version, storage size and other product data required to identify the specific NTAG21x.

This command is also available on other NTAG products to have a common way of identifying products across platforms and evolution steps.

The GET_VERSION command has no arguments and replies the version information for the specific NTAG21x type. The command structure is shown in Figure 11 and Table 17.

Table 18 shows the required timing.

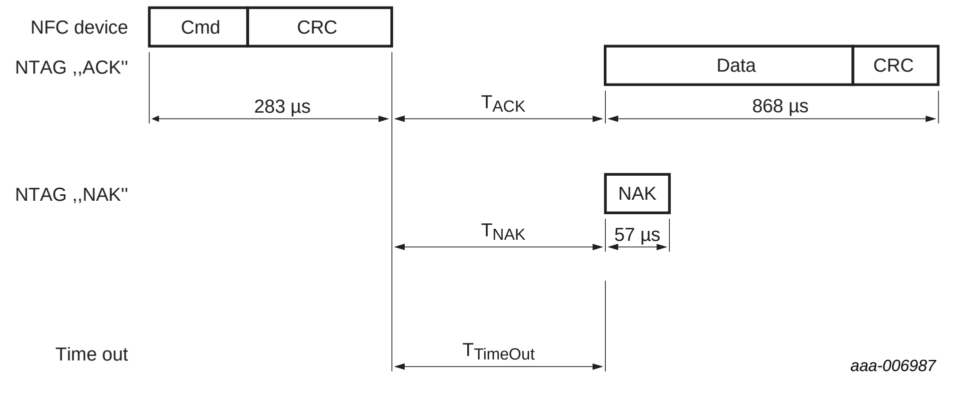


Fig 11. GET_VERSION command

Table 17. GET_VERSION command

Name	Code	Description	Length
Cmd	60h	Get product version	1 byte
CRC	-	CRC according to Ref. 1	2 bytes
Data	-	Product version information, s	8 bytes
NAK	see Table 14	see Section 9.3	4-bit

Table 18. GET_VERSION timing

These times exclude the end of communication of the NFC device.

	$T_{ACK/NACK}$ min	$T_{ACK/NACK}$ max	$T_{TimeOut}$
GET_VERSION	n=9[1]	$T_{TimeOut}$	5 ms

[1] Refer to Section 9.2 "Timings".

Table 19. GET_VERSION response for NTAG210 and NTAG212

Byte no.	Description	NTAG210	NTAG212	Interpretation
0	fixed Header	00h	00h	
1	vendor ID	04h	04h	NXP Semiconductors
2	product type	04h	04h	NTAG
3	product subtype	01h	01h	17 pF
4	major product version	01h	01h	1
5	minor product version	00h	00h	V0
6	storage size	0Bh	0Eh	see following information
7	protocol type	03h	03h	ISO/IEC 14443-3 compliant

The most significant 7 bits of the storage size byte are interpreted as a unsigned integer value n. As a result, it codes the total available user memory size as 2^n. If the least significant bit is 0b, the user memory size is exactly 2^n. If the least significant bit is 1b, the user memory size is between 2^n and 2^{n+1}.

The user memory for NTAG210 is 48 bytes. This memory size is between 32 bytes and 64 bytes. Therefore, the most significant 7 bits of the value 0Bh, are interpreted as 5d and the least significant bit is 1b.

The user memory for NTAG212 is 128 bytes. This memory size is exactly 128 bytes. Therefore, the most significant 7 bits of the value 0Eh, are interpreted as 7d and the least significant bit is 0b.

10.2 READ

The READ command requires a start page address, and returns the 16 bytes of four NTAG21x pages. For example, if address (Addr) is 03h then pages 03h, 04h, 05h, 06h are returned. Special conditions apply if the READ command address is near the end of the accessible memory area. The special conditions also apply if at least part of the addressed pages is within a password protected area. For details on those cases and the command structure refer to Figure 11 and Table 17.

Table 21 shows the required timing.

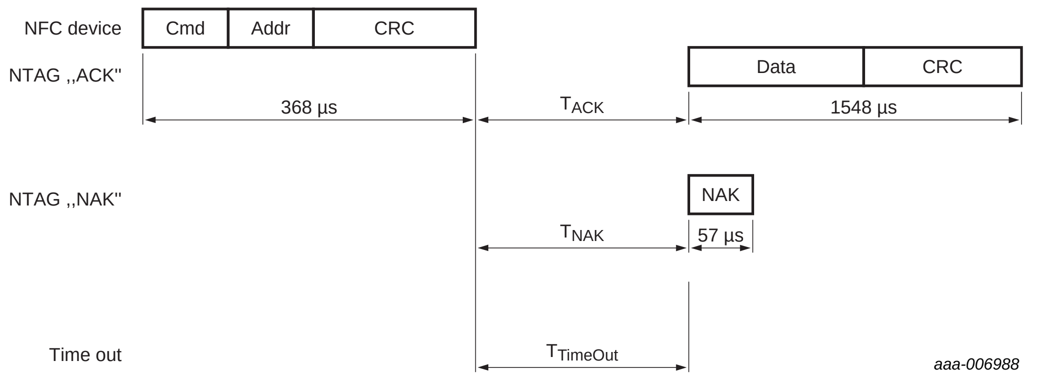


Fig 12. READ command

Table 20. READ command

Name	Code	Description	Length
Cmd	30h	read four pages	1 byte
Addr	-	start page address	1 byte
CRC	-	CRC according to Ref. 1	2 bytes
Data	-	Data content of the addressed pages	16 bytes
NAK	see Table 14	see Section 9.3	4-bit

Table 21. READ timing

These times exclude the end of communication of the NFC device.

	$T_{ACK/NACK}$ min	$T_{ACK/NACK}$ max	$T_{TimeOut}$
READ	n=9[1]	$T_{TimeOut}$	5 ms

[1] Refer to Section 9.2 “Timings”.

In the initial state of NTAG21x, all memory pages are allowed as Addr parameter to the READ command.

- page address 00h to 13h for NTAG210
- page address 00h to 28h for NTAG212

Addressing a memory page beyond the limits above results in a NAK response from NTAG21x.

A roll-over mechanism is implemented to continue reading from page 00h once the end of the accessible memory is reached. Reading from address 11h on a NTAG210 results in pages 11h, 12h, 13h and 00h being returned.

The following conditions apply if part of the memory is password protected for read access:

- if NTAG21x is in the ACTIVE state
  - addressing a page which is equal or higher than AUTH0 results in a NAK response
  - addressing a page lower than AUTH0 results in data being returned with the roll-over mechanism occurring just before the AUTH0 defined page
- if NTAG21x is in the AUTHENTICATED state
  - the READ command behaves like on a NTAG21x without access protection

Remark: PWD and PACK values can never be read out of the memory. When reading from the pages holding those two values, all 00h bytes are replied to the NFC device instead.

10.3 FAST_READ

The FAST_READ command requires a start page address and an end page address and returns the all n*4 bytes of the addressed pages. For example if the start address is 03h and the end address is 07h then pages 03h, 04h, 05h, 06h and 07h are returned. If the addressed page is outside of accessible area, NTAG21x replies a NAK. For details on those cases and the command structure, refer to Figure 13 and Table 22.

Table 23 shows the required timing.

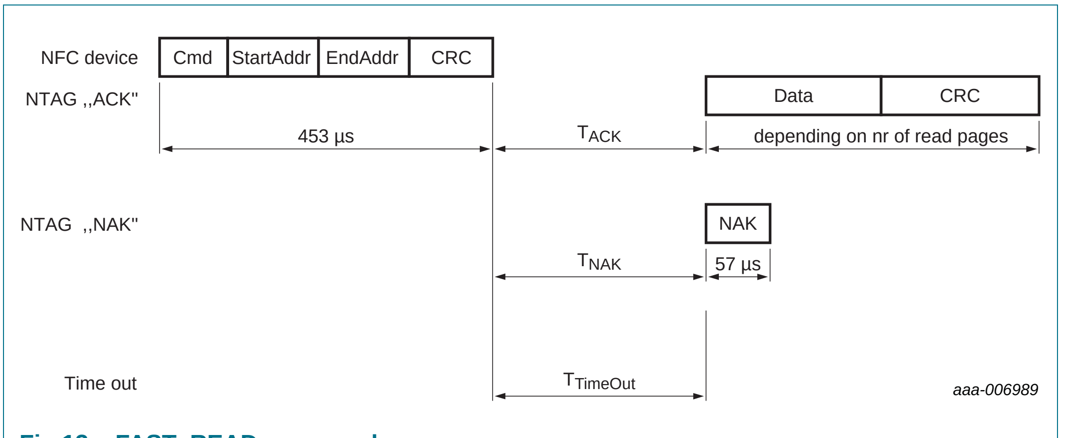


Fig 13. FAST_READ command

Table 22. FAST_READ command

Name	Code	Description	Length
Cmd	3Ah	read multiple pages	1 byte
StartAddr	-	start page address	1 byte
EndAddr	-	end page address	1 byte
CRC	-	CRC according to Ref. 1	2 bytes
Data	-	data content of the addressed pages	n*4 bytes
NAK	see Table 14	see Section 9.3	4-bit

Table 23. FAST_READ timing

These times exclude the end of communication of the NFC device.

	$T_{ACK/NACK}$ min	$T_{ACK/NACK}$ max	$T_{TimeOut}$
FAST_READ	n=9[1]	$T_{TimeOut}$	5 ms

[1] Refer to Section 9.2 “Timings”.

In the initial state of NTAG21x, all memory pages are allowed as StartAddr parameter to the FAST_READ command.

- page address 00h to 13h for NTAG210
- page address 00h to 28h for NTAG212

Addressing a memory page beyond the limits above results in a NAK response from NTAG21x.

The EndAddr parameter must be equal to or higher than the StartAddr.

The following conditions apply if part of the memory is password protected for read access:

- if NTAG21x is in the ACTIVE state
    - if any requested page address is equal or higher than AUTH0 a NAK is replied
- if NTAG21x is in the AUTHENTICATED state
    - the FAST_READ command behaves like on a NTAG21x without access protection

Remark: PWD and PACK values can never be read out of the memory. When reading from the pages holding those two values, all 00h bytes are replied to the NFC device instead.

Remark: The FAST_READ command is able to read out the whole memory with one command. Nevertheless, receive buffer of the NFC device must be able to handle the requested amount of data as there is no chaining possibility.

10.4 WRITE

The WRITE command requires a block address, and writes 4 bytes of data into the addressed NTAG21x page. The WRITE command is shown in Figure 14 and Table 24.

Table 25 shows the required timing.

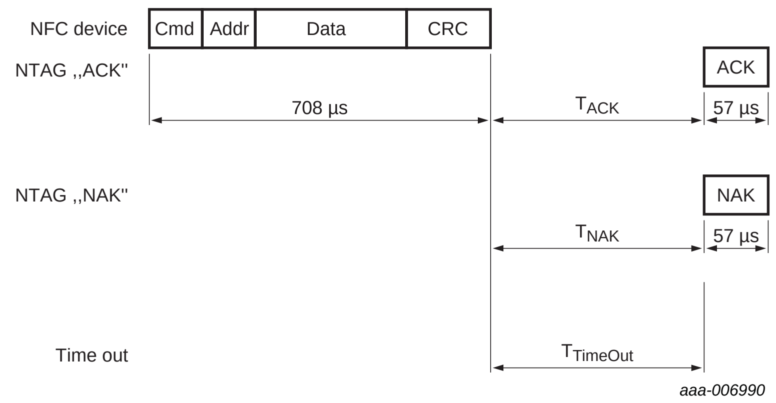


Fig 14. WRITE command

Table 24. WRITE command

Name	Code	Description	Length
Cmd	A2h	write one page	1 byte
Addr	-	page address	1 byte
CRC	-	CRC according to Ref. 1	2 bytes
Data	-	data	4 bytes
NAK	see Table 14	see Section 9.3	4-bit

Table 25. WRITE timing

These times exclude the end of communication of the NFC device.

	$T_{ACK/NACK}$ min	$T_{ACK/NACK}$ max	$T_{TimeOut}$
WRITE	n=9[1]	$T_{TimeOut}$	10 ms

[1] Refer to Section 9.2 “Timings”.

In the initial state of NTAG21x, the following memory pages are valid Addr parameters to the WRITE command.

- page address 02h to 13h for NTAG210
- page address 02h to 28h for NTAG212

Addressing a memory page beyond the limits above results in a NAK response from NTAG21x.

Pages which are locked against writing cannot be reprogrammed using any write command. The locking mechanisms include static and dynamic lock bits as well as the locking of the configuration pages.

The following conditions apply if part of the memory is password protected for write access:

- if NTAG21x is in the ACTIVE state
    - writing to a page which address is equal or higher than AUTH0 results in a NAK response
- if NTAG21x is in the AUTHENTICATED state
    - the WRITE command behaves like on a NTAG21x without access protection

NTAG21x features tearing protected write operations to specific memory content. The following pages are protected against tearing events during a WRITE operation:

- page 2 containing static lock bits
- page 3 containing CC bits
- page 36 containing the additional dynamic lock bits for the NTAG212

10.5 COMPATIBILITY_WRITE

The COMPATIBILITY_WRITE command is implemented to guarantee interoperability with the established MIFARE Classic PCD infrastructure, in case of coexistence of ticketing and NFC applications. Even though 16 bytes are transferred to NTAG21x, only the least significant 4 bytes (bytes 0 to 3) are written to the specified address. Set all the remaining bytes, 04h to 0Fh, to logic 00h. The COMPATIBILITY_WRITE command is shown in Figure 15, Figure 16 and Table 24.

Table 27 shows the required timing.

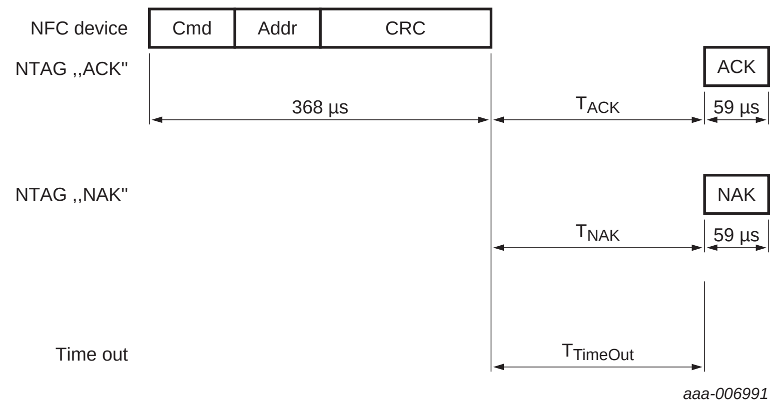


Fig 15. COMPATIBILITY_WRITE command part 1

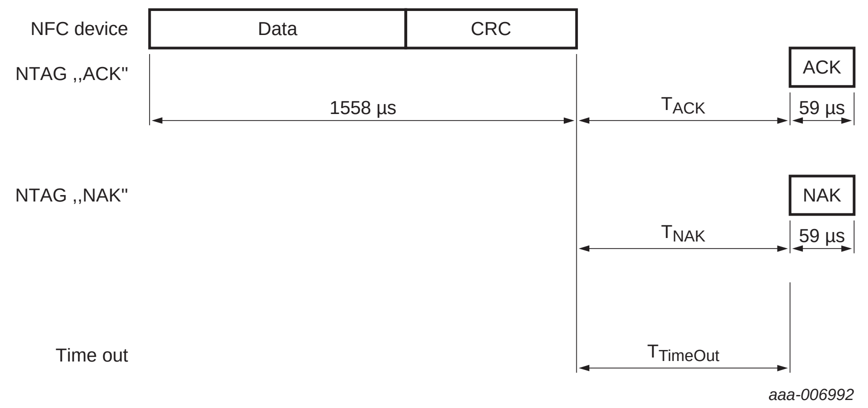


Fig 16. COMPATIBILITY_WRITE command part 2

Table 26. COMPATIBILITY_WRITE command

Name	Code	Description	Length
Cmd	A0h	compatibility write	1 byte
Addr	-	page address	1 byte
CRC	-	CRC according to Ref. 1	2 bytes
Data	-	16-byte Data, only least significant 4 bytes are written	16 bytes
NAK	see Table 14	see Section 9.3	4-bit

Table 27. COMPATIBILITY_WRITE timing

These times exclude the end of communication of the NFC device.

	$T_{ACK/NACK}$ min	$T_{ACK/NACK}$ max	$T_{TimeOut}$
COMPATIBILITY_WRITE part 1	n=9[1]	$T_{TimeOut}$	5 ms
COMPATIBILITY_WRITE part 2	n=9[1]	$T_{TimeOut}$	10 ms

[1] Refer to Section 9.2 "Timings".

In the initial state of NTAG21x, the following memory pages are valid Addr parameters to the COMPATIBILITY_WRITE command.

- page address 02h to 13h for NTAG210
- page address 02h to 28h for NTAG212

Addressing a memory page beyond the limits above results in a NAK response from NTAG21x.

Pages which are locked against writing cannot be reprogrammed using any write command. The locking mechanisms include static and dynamic lock bits as well as the locking of the configuration pages.

The following conditions apply if part of the memory is password protected for write access:

- if NTAG21x is in the ACTIVE state
  - writing to a page which address is equal or higher than AUTH0 results in a NAK response
- if NTAG21x is in the AUTHENTICATED state
  - the COMPATIBILITY_WRITE command behaves the same as on a NTAG21x without access protection

NTAG21x features tearing protected write operations to specific memory content. The following pages are protected against tearing events during a COMPATIBILITY_WRITE operation:

- page 2 containing static lock bits
- page 3 containing CC bits
- page 36 containing the additional dynamic lock bits for the NTAG212

10.6 PWD_AUTH

A protected memory area can be accessed only after a successful password verification using the PWD_AUTH command. The AUTH0 configuration byte defines the protected area. It specifies the first page that the password mechanism protects. The level of protection can be configured using the PROT bit either for write protection or read/write protection. The PWD_AUTH command takes the password as parameter and, if successful, returns the password authentication acknowledge, PACK. By setting the AUTHLIM configuration bits to a value larger than 000b, the number of unsuccessful password verifications can be limited. Each unsuccessful authentication is then counted in a counter featuring anti-tearing support. After reaching the limit of unsuccessful attempts, the memory access specified in PROT, is no longer possible. The PWD_AUTH command is shown in Figure 17 and Table 28.

Table 29 shows the required timing.

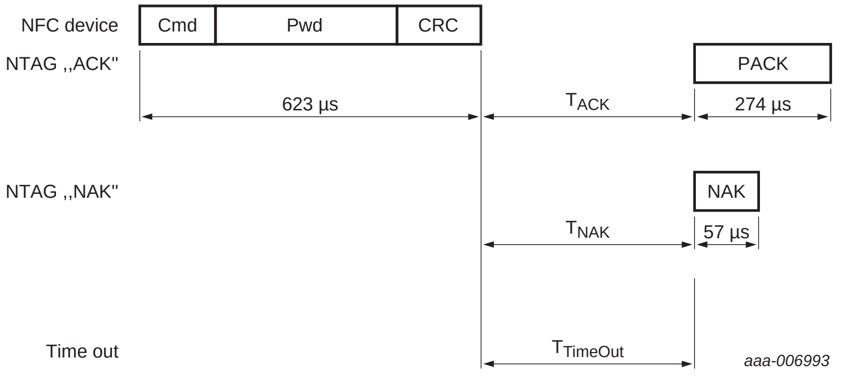


Fig 17. PWD_AUTH command

Table 28. PWD_AUTH command

Name	Code	Description	Length
Cmd	1Bh	password authentication	1 byte
Pwd	-	password	4 bytes
CRC	-	CRC according to Ref. 1	2 bytes
PACK	-	password authentication acknowledge	2 bytes
NAK	see Table 14	see Section 9.3	4-bit

Table 29. PWD_AUTH timing
These times exclude the end of communication of the NFC device.

	$T_{ACK/NACK}$ min	$T_{ACK/NACK}$ max	$T_{TimeOut}$
PWD_AUTH	n=9[1]	$T_{TimeOut}$	5 ms

[1] Refer to Section 9.2 “Timings”.

Remark: It is strongly recommended to change the password from its delivery state at tag issuing and set the AUTH0 value to the PWD page.

10.7 READ_SIG

The READ_SIG command returns an IC specific, 32-byte ECC signature, to verify NXP Semiconductors as the silicon vendor. The signature is programmed at chip production and cannot be changed afterwards. The command structure is shown in Figure 18 and Table 30.

Table 31 shows the required timing.

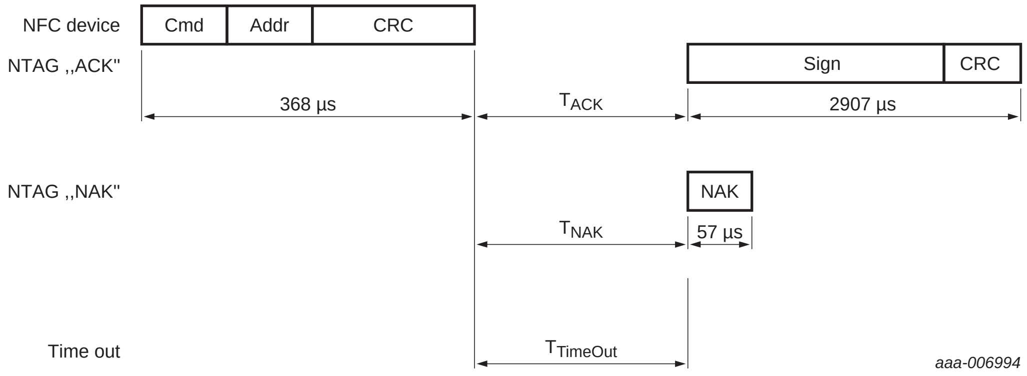


Fig 18. READ_SIG command

Table 30. READ_SIG command

Name	Code	Description	Length
Cmd	3Ch	read ECC signature	1 byte
Addr	00h	RFU, is set to 00h	1 byte
CRC	-	CRC according to Ref. 1	2 bytes
Signature	-	ECC signature	32 bytes
NAK	see Table 14	see Section 9.3	4 bit

Table 31. READ_SIG timing

These times exclude the end of communication of the NFC device.

	$T_{ACK/NACK}$ min	$T_{ACK/NACK}$ max	$T_{TimeOut}$
READ_SIG	n=9[1]	$T_{TimeOut}$	5 ms

[1] Refer to Section 9.2 “Timings”.

Details on how to check the signature value are provided in the following Application note (Ref. 5). It is foreseen to offer an online and offline way to verify originality of NTAG21x.

11. Limiting values

Stresses exceeding one or more of the limiting values can cause permanent damage to the device. Exposure to limiting values for extended periods can affect device reliability.

Table 32. Limiting values
In accordance with the Absolute Maximum Rating System (IEC 60134).

Symbol	Parameter		Min	Max	Unit
I_I	input current		-	40	mA
P_{tot}	total power dissipation		-	120	mW
T_{stg}	storage temperature		–55	125	°C
T_{amb}	ambient temperature		–25	70	°C
V_{ESD}	electrostatic discharge voltage on LA/LB	[1]	2	-	kV

[1] ANSI/ESDA/JEDEC JS-001; Human body model: C = 100 pF, R = 1.5 kΩ

12. Characteristics

Table 33. Characteristics

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
C_i	input capacitance		[1]	-	17.0	-	pF
f_i	input frequency			-	13.56	-	MHz
EEPROM characteristics							
t_{ret}	retention time	T_{amb} = 22 °C		10	-	-	year
$N_{endu(W)}$	write endurance	T_{amb} = 22 °C		100.000	-	-	cycle

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

13. Wafer specification

For more details on the wafer delivery forms see Ref. 5.

Table 34. Wafer specifications NTAG210

Wafer	
diameter	200 mm typical (8 inches)
maximum diameter after foil expansion	210 mm
thickness	
NT2L1011G0DUD and NT2L1211G0DUD	120 µm ± 15 µm
NT2L1011G0DUF and NT2L1211G0DUF	75 µm ± 10 µm
flatness	not applicable
Potential Good Dies per Wafer (PGDW)	103682
Wafer backside	
material	Si
treatment	ground and stress relieve
roughness	R_a max = 0.5 µm
	R_t max = 5 µm
Chip dimensions	
step size[1]	x = 505 µm
	y = 590 µm
gap between chips[1]	typical = 20 µm
	minimum = 5 µm
Passivation	
type	sandwich structure
material	PSG / nitride
thickness	500 nm / 600 nm
Au bump (substrate connected to VSS)	
material	> 99.9 % pure Au
hardness	35 to 80 HV 0.005
shear strength	> 70 MPa
height	18 µm
height uniformity	within a die = ±2 µm
	within a wafer = ±3 µm
	wafer to wafer = ±4 µm
flatness	minimum = ±1.5 µm
size	LA, LB, GND, TP[2] = 60 µm × 60 µm
size variation	±5 µm
under bump metallization	sputtered TiW

[1] The step size and the gap between chips may vary due to changing foil expansion

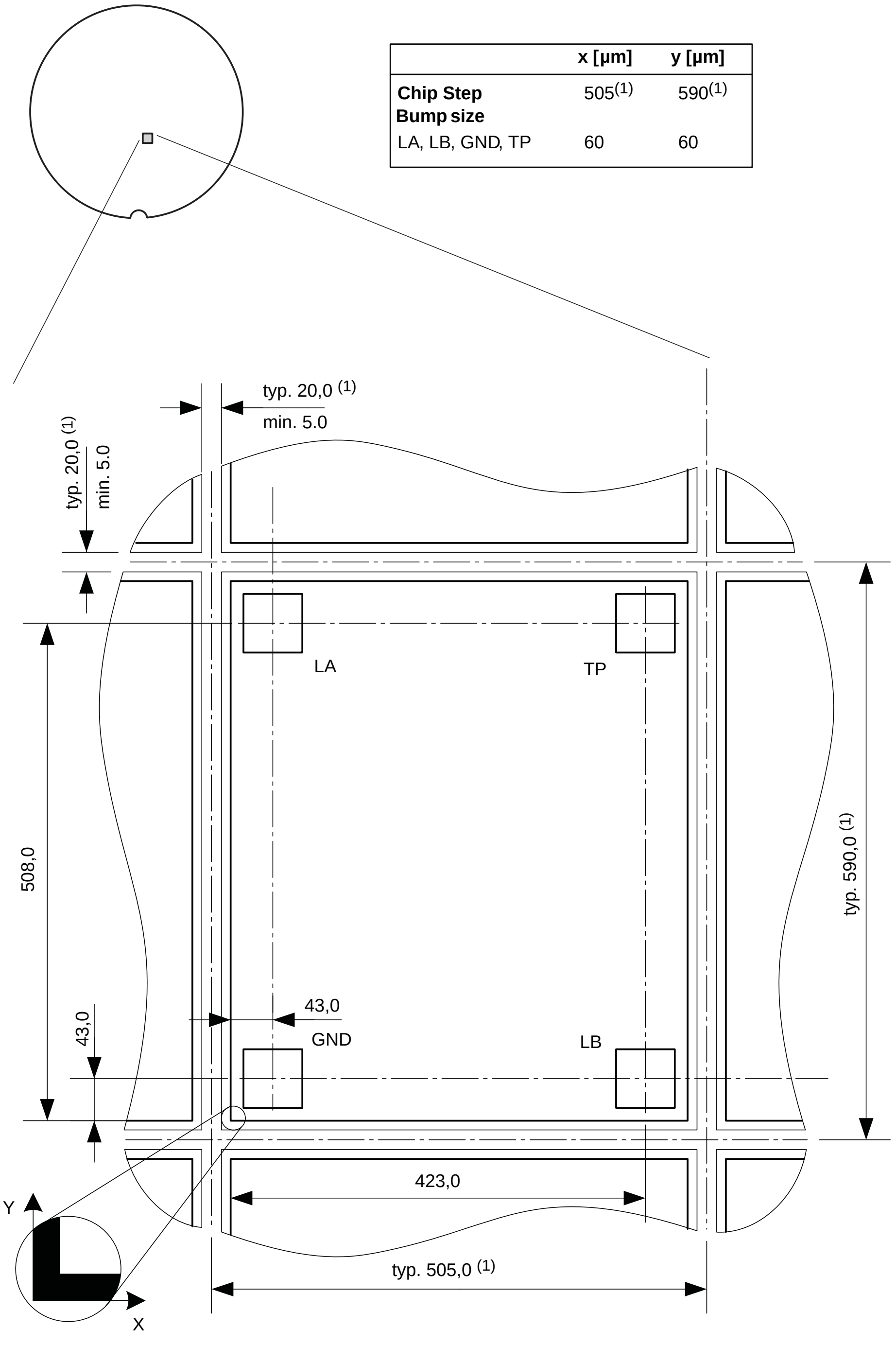
[2] Pads GND and TP are disconnected when wafer is sawn

13.1 Fail die identification

Electronic wafer mapping covers the electrical test results and additionally the results of mechanical/visual inspection. No ink dots are applied.

13.2 Bare die outline

For more details on the wafer delivery forms see Ref. 5.



	x [µm]	y [µm]
Chip Step	505(1)	590(1)
Bump size		
LA, LB, GND, TP	60	60

(1) the air gap and thus the step size may vary due to varying foil expansion

(2) all dimensions in µm, pad locations measured from metal ring edge (see detail)

aaa-006995

Fig 19. Bare die outline NTAG210/212

14. Abbreviations

Table 35. Abbreviations and symbols

Acronym	Description
ACK	ACKnowledge
ATQA	Answer To reQuest, Type A
CRC	Cyclic Redundancy Check
CC	Capability container
CT	Cascade Tag (value 88h) as defined in ISO/IEC 14443-3 Type A
ECC	Elliptic Curve Cryptography
EEPROM	Electrically Erasable Programmable Read-Only Memory
FDT	Frame Delay Time
FFC	Film Frame Carrier
IC	Integrated Circuit
LCR	L = inductance, Capacitance, Resistance (LCR meter)
LSB	Least Significant Bit
NAK	Not AcKnowledge
NFC device	NFC Forum device
NFC tag	NFC Forum tag
NV	Non-Volatile memory
REQA	REQuest command, Type A
RF	Radio Frequency
RFUI	Reserver for Future Use - Implemented
RMS	Root Mean Square
SAK	Select AcKnowledge, type A
SECS-II	SEMI Equipment Communications Standard part 2
TiW	Titanium Tungsten
UID	Unique IDentifier
WUPA	Wake-Up Protocol type A

15. References

[1] **ISO/IEC 14443 —** International Organization for Standardization

[2] **NFC Forum Tag 2 Type Operation, Technical Specification —** NFC Forum, 31.05.2011, Version 1.1

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

[4] **AN11276 NTAG Antenna Design Guide —** Application note, BU-ID Document number 2421**[1]

[5] **AN11350 NTAG21x Originality Signature Validation —** Application note, BU-ID Document number 2604**

[6] **General specification for 8" wafer on UV-tape; delivery types —** Delivery Type Description, BU-ID Document number 1005**

[7] **Certicom Research. SEC 2 —** Recommended Elliptic Curve Domain Parameters, version 2.0, January 2010

---

[1] ** ... BU ID document version number

16. Revision history

Table 36. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
NTAG210_212 v.3.0	20130314	Product data sheet	-	NTAG210_242320
Modifications:	• Editorial changes • Security status changed into COMPANY PUBLIC			
NTAG210_242320	20121219	Preliminary data sheet	-	-
	• Initial version			

17. Legal information

17.1 Data sheet status

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

[1] Please consult the most recently issued document before initiating or completing a design.

[2] The term ‘short data sheet’ is explained in section “Definitions”.

[3] The product status of device(s) described in this document may have changed since this document was published and may differ in case of multiple devices. The latest product status information is available on the Internet at URL http://www.nxp.com.

17.2 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

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

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

17.3 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors’ aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the *Terms and conditions of commercial sale* of NXP Semiconductors.

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

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

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer’s sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer’s applications and products planned, as well as for the planned application and use of customer’s third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer’s applications or products, or the application or use by customer’s third party customer(s). Customer is responsible for doing all necessary testing for the customer’s applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer’s third party customer(s). NXP does not accept any liability in this respect.

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

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer’s general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

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

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

Quick reference data — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

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.

17.4 Licenses

Purchase of NXP ICs with NFC technology

Purchase of an NXP Semiconductors IC that complies with one of the Near Field Communication (NFC) standards ISO/IEC 18092 and ISO/IEC 21481 does not convey an implied license under any patent right infringed by implementation of any of those standards.

17.5 Trademarks

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

MIFARE — is a trademark of NXP B.V.

18. Contact information

For more information, please visit: http://www.nxp.com

For sales office addresses, please send an email to: salesaddresses@nxp.com

19. Tables

20. Figures

21. Contents

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

Date of release: 14 March 2013
242330

Компания «ЭлектроПласт» предлагает заключение долгосрочных отношений при поставках импортных электронных компонентов на взаимовыгодных условиях!

Наши преимущества:

- Оперативные поставки широкого спектра электронных компонентов отечественного и импортного производства напрямую от производителей и с крупнейших мировых складов;
- Поставка более 17-ти миллионов наименований электронных компонентов;
- Поставка сложных, дефицитных, либо снятых с производства позиций;
- Оперативные сроки поставки под заказ (от 5 рабочих дней);
- Экспресс доставка в любую точку России;
- Техническая поддержка проекта, помощь в подборе аналогов, поставка прототипов;
- Система менеджмента качества сертифицирована по Международному стандарту ISO 9001;
- Лицензия ФСБ на осуществление работ с использованием сведений, составляющих государственную тайну;
- Поставка специализированных компонентов (Xilinx, Altera, Analog Devices, Intersil, Interpoint, Microsemi, Aeroflex, Peregrine, Syfer, Eurofarad, Texas Instrument, Miteq, Cobham, E2V, MA-COM, Hittite, Mini-Circuits,General Dynamics и др.);

Помимо этого, одним из направлений компании «ЭлектроПласт» является направление «Источники питания». Мы предлагаем Вам помощь Конструкторского отдела:

- Подбор оптимального решения, техническое обоснование при выборе компонента;
- Подбор аналогов;
- Консультации по применению компонента;
- Поставка образцов и прототипов;
- Техническая поддержка проекта;
- Защита от снятия компонента с производства.

Как с нами связаться

Телефон: 8 (812) 309 58 32 (многоканальный)
Факс: 8 (812) 320-02-42
Электронная почта: org@eplast1.ru
Адрес: 198099, г. Санкт-Петербург, ул. Калинина, дом 2, корпус 4, литера А.