

NTAG213F/216F

NFC Forum Type 2 Tag compliant IC with 144/888 bytes user memory and field detection

Rev. 3.0 — 18 July 2013
262230

Product data sheet
COMPANY PUBLIC

1. General description

The NTAG213F and NTAG216F are the new NFC forum compliant Type 2 tag products developed by NXP Semiconductors for applications in electronics (i.e. connection handover, Bluetooth simple pairing, Wi-Fi Protected set-up, device authentication, gaming and others) - see [Figure 1](#).

On top of offering a large range of User memory (144bytes for NTAG213F and 888bytes for NTAG216F), the NTAG21xF product family offers innovative functionalities like configuration of the field detection, the SLEEP mode, the FAST_READ command and a configurable password protection.

The NTAG21xF product family is designed to fully comply to NFC Forum Type 2 Tag ([Ref. 2](#)) and ISO/IEC14443 Type A ([Ref. 1](#)) specifications.

The NTAG21xF product family also offers the same package (HXSON4), the same input capacitance and a full pinning compatibility to the NTAG203F product.

1.1 Contactless energy and data transfer

Communication to NTAG21xF can be established only when the IC is connected to an antenna. Form and specification of the antenna is out of scope of this document.

When NTAG21xF 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.

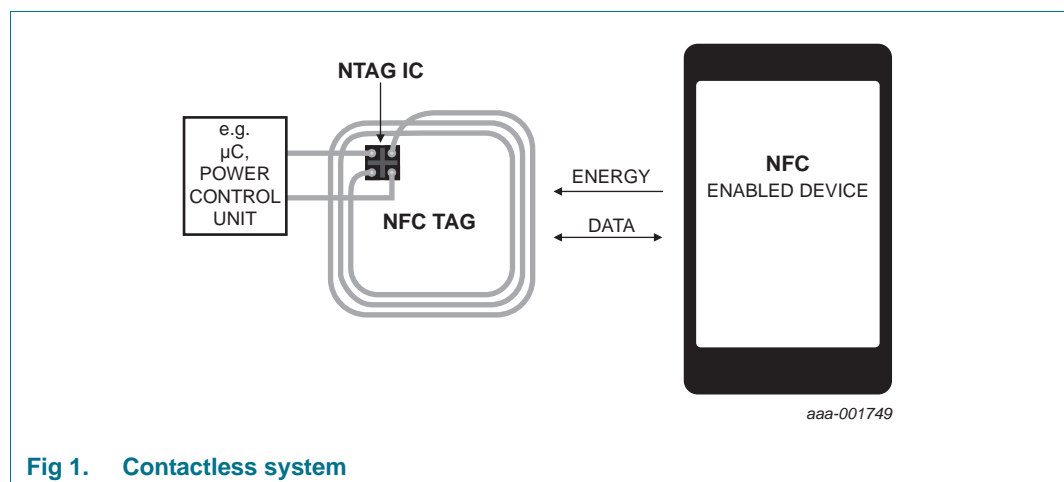


Fig 1. Contactless system



1.2 Simple deployment and user convenience

NTAG21xF 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 communication time overhead
- The improved RF performance allows for more flexibility in the choice of shape, dimension and materials
- The HXSON4 package delivery form is the same one used as the NTAG203F with the same pinning
- The field detect functionality is based on an open-drain implementation that requires only one pull up resistor

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 up to 0Fh page (per 2 pages (NTAG 213F) or per 16 pages (NTAG 216F) for the extended memory section)
- ECC based originality signature
- 32-bit password protection to prevent unauthorized memory operations

1.4 Field detection

The NTAG21xF product family features an RF field detection functionality based on Open Drain (see Figure 2) that can be configured with different RF signal or actions trigger:

- upon any RF field presence
- upon the first Start-of-Frame (start of the communication)
- upon the selection of the tag

The corresponding output signal can be used as interrupt source to e.g. wake up an embedded microcontroller or trigger further actions - e.g. Bluetooth and WiFi pairing. For more information on this feature, please refer to Ref. 8.

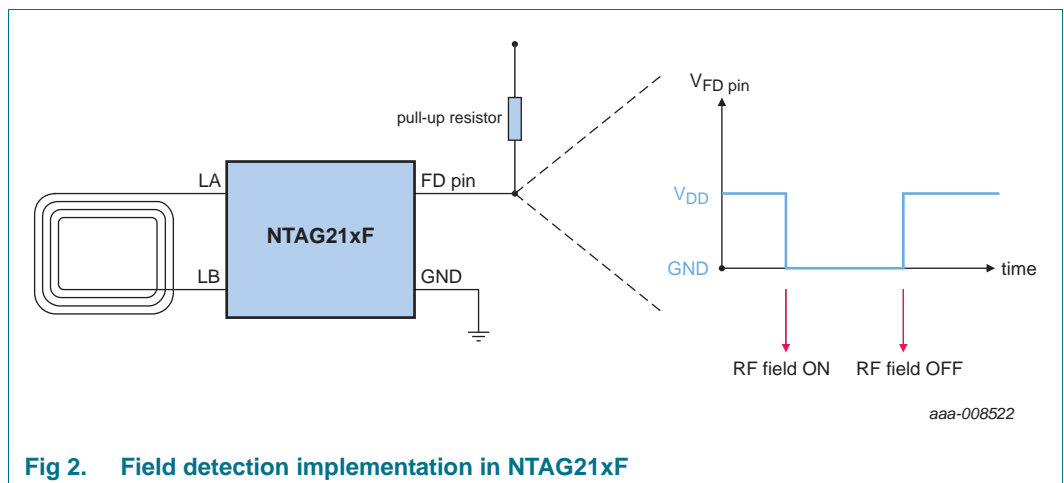


Fig 2. Field detection implementation in NTAG21xF

1.5 Sleep mode

The NTAG21xF product family offers the SLEEP mode feature which allows the electronic device connected with the NTAG21xF to disable the NTAG21xF product by shorting the field detect pin to ground followed by RF field reset. This enables the electronic device to hide the NTAG21xF product from the NFC reader device in case e.g. its battery level is too low or for privacy reason.

1.6 NFC Forum Tag 2 Type compliance

NTAG21xF 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](#)).

1.7 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)
- True anticollision
- ECC based originality signature
- Fast read command
- UID ASCII mirror for automatic serialization NDEF messages
- Automatic NFC counter triggered at read command
- NFC counter ASCII mirror for automatic adding actual read counter value to the NDEF message
- Configurable Field detect pin with open drain implementation
- SLEEP mode to disable or re-enable the NTAG21xF device from the connected electronics device side

2.1 EEPROM

- 180 or 924 bytes organized in 45 or 231 pages with 4 bytes per page
- 144 or 888 bytes freely available user Read/Write area (36 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 NTAG213F or per 16 pages for NTAG216F
- 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

- Goods and device authentication
- Call request
- SMS
- Call to action
- Bluetooth pairing
- WiFi pairing
- Connection handover

4. Ordering information

Table 1. Ordering information

Type number	Package		Version
	Name	Description	
NT2H1611F0DTL	HXSON4	Plastic leadless module carrier package; 35 mm wide tape 888 bytes user memory, 50pF input capacitance	-
NT2H1311F0DTL	HXSON4	Plastic leadless module carrier package; 35 mm wide tape 144 bytes user memory, 50pF input capacitance	-

5. Block diagram

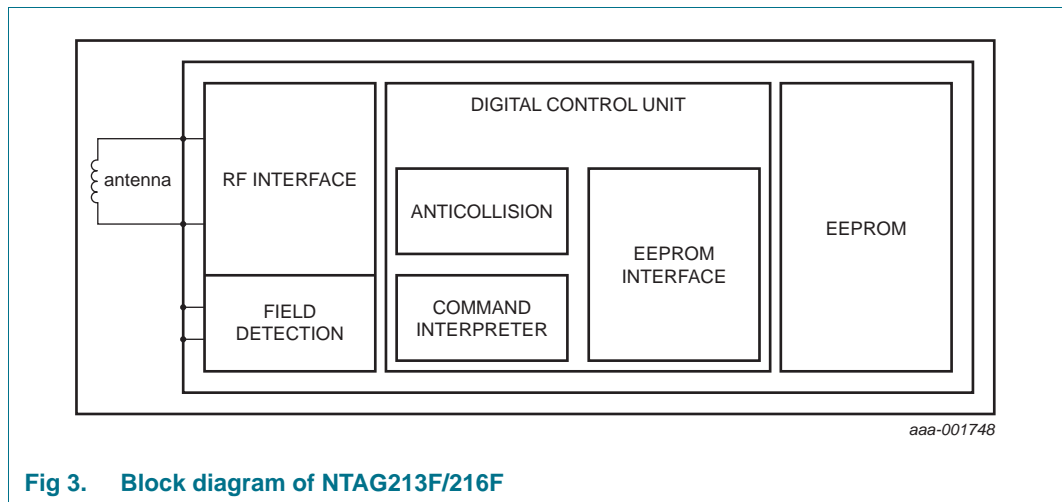


Fig 3. Block diagram of NTAG213F/216F

6. Pinning information

6.1 Pinning

The pinning of the NTAG21xF is exactly the same as for the NTAG203F.

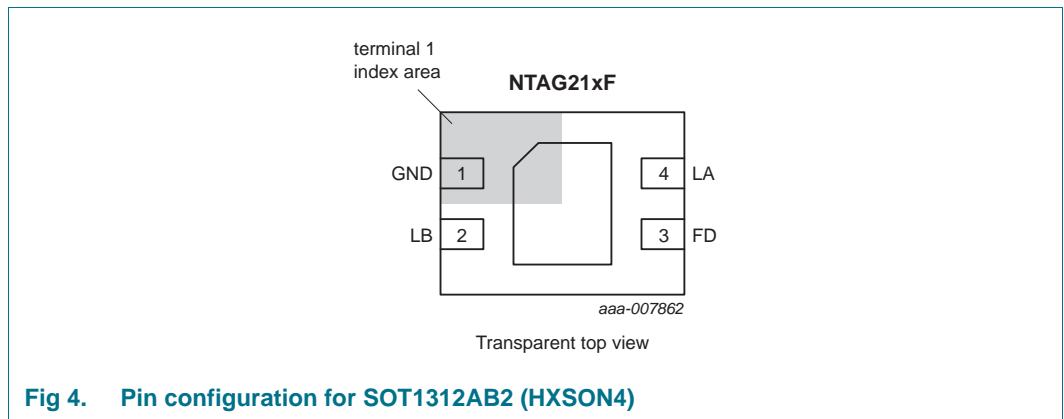


Fig 4. Pin configuration for SOT1312AB2 (HXSON4)

Table 2. Pin description of the HXSON4 package

Contactless interface module		NTAG213F NTAG216F
Antenna contacts	Symbol	Description
Pin 1	GND	Ground
Pin 2	LB	Antenna connection LB
Pin 3	FD	RF Field Detect connection
Pin 4	LA	Antenna connection LA

It is recommended to leave the central pad of the package floating.

7. Marking

7.1 Marking HXSON4

Table 3. Marking HXSON4

Type number	Description	
NT2H1301F0DTL	Marking Line A	N3F
	Marking Line B	yww
NT2H1601F0DTL	Marking Line A	N2F
	Marking Line B	yww

8. Functional description

8.1 Block description

NTAG21xF ICs consist of a 180 (NTAG213F) or 924 bytes (NTAG216F) EEPROM, RF interface and Digital Control Unit. Energy and data are transferred via an antenna consisting of a coil with a few turns which is directly connected to NTAG21xF. 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 tags may be selected and managed in sequence
- Command interpreter: processes memory access commands supported by the NTAG21xF
- EEPROM interface
- NTAG213F 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
- NTAG216F 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 data 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 = $16 \times 9 + 2 \times 9 + 1$ start bit). The maximum length of a fixed size tag to NFC device frame is 307 bits (32 data bytes + 2 CRC bytes = $32 \times 9 + 2 \times 9 + 1$ 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.

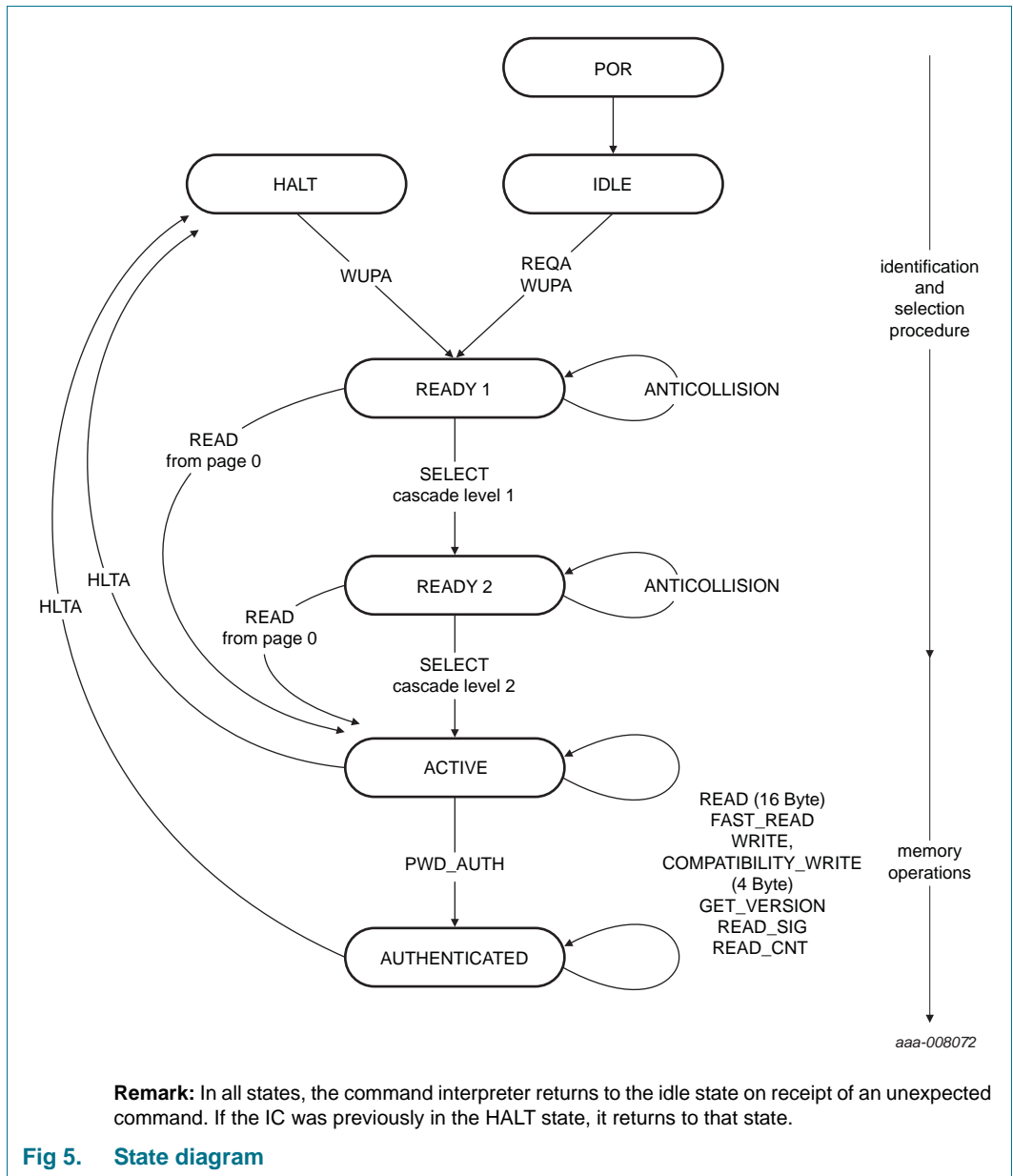
8.3 Data integrity

Following mechanisms are implemented in the contactless communication link between NFC device and the NTAG21xF to ensure 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 NTAG21xF. The command response is depending on the communication state of the IC and for memory operations also on the access limitations valid for the corresponding page.



8.4.1 IDLE state

After a power-on reset (POR), NTAG21xF 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 NTAG21xF 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 NTAG21xF into READY2 state where the second part of the UID is resolved.
- READ command (from address 0): all anticollision mechanisms are bypassed and the NTAG21xF 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 NTAG21xF 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 NTAG21xF returns to the IDLE or HALT state.

8.4.3 READY2 state

In this state, NTAG21xF 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 NTAG21xF 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. NTAG21xF 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 NTAG21xF is in the NFC device field, a READ command from address 0 selects all NTAG21xF 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 NTAG21xF 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 NTAG21xF 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 NTAG21xF returns to either the IDLE state or HALT state.

NTAG21xF transits to the AUTHENTICATED state after successful password verification using the PWD_AUTH command.

8.4.5 AUTHENTICATED state

In this state, all memory operations as well as 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 NTAG21xF 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 NTAG21xF 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 NTAG21xF. An already processed NTAG21xF 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. NTAG21xF 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 NTAG21xF state remains unchanged.

8.5 Memory organization

The EEPROM memory is organized in pages with 4 bytes per page. NTAG213F variant has 45 pages and NTAG216F variant has 231 pages in total. The memory organization can be seen in [Figure 6](#) and [Figure 7](#), the functionality of the different memory sections is described in the following sections.

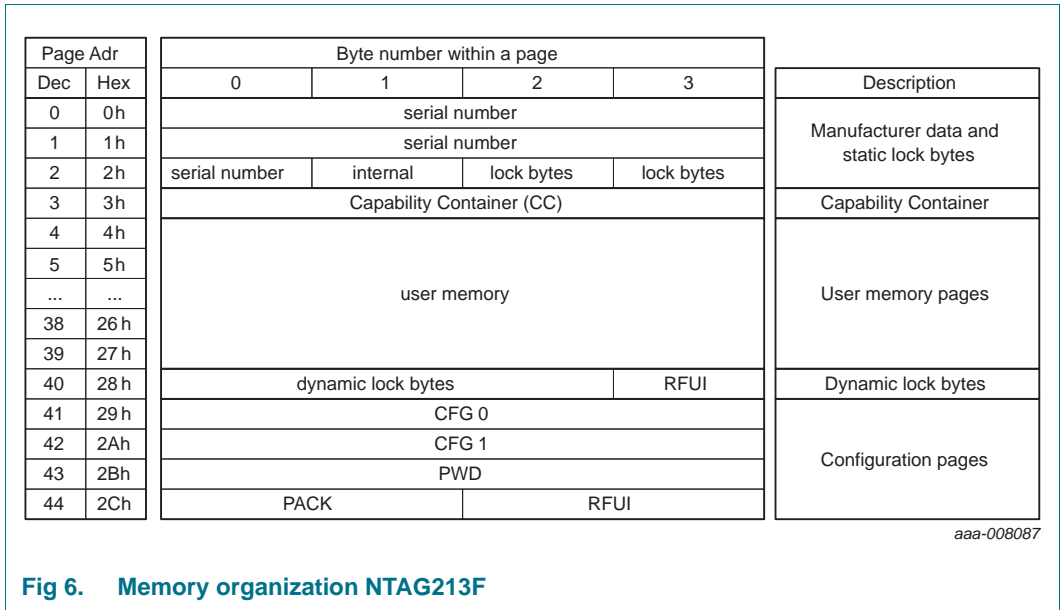


Fig 6. Memory organization NTAG213F

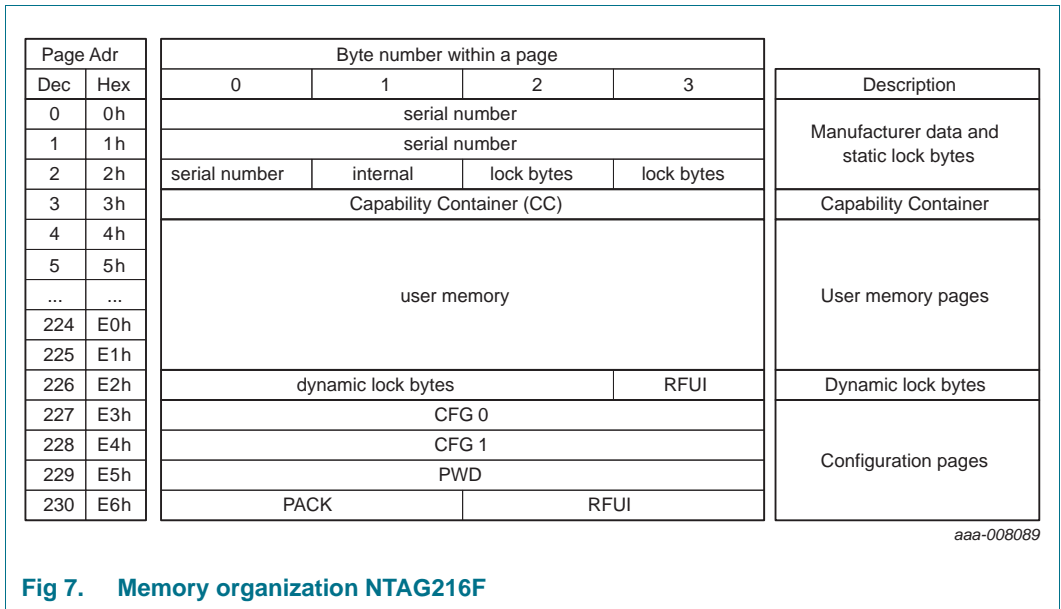


Fig 7. Memory organization NTAG216F

The structure of manufacturing data, static lock bytes, capability container and user memory pages (except of the user memory length) are compatible to NTAG203F.

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.

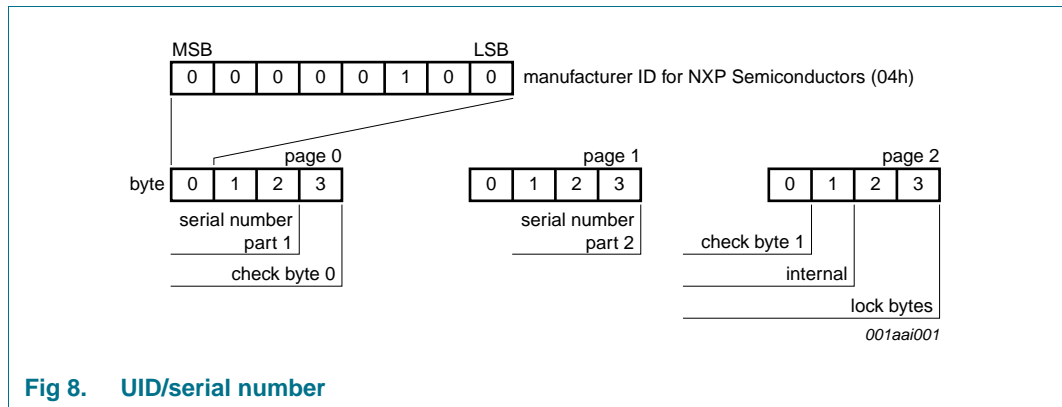


Fig 8. UID/serial number

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

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

8.5.2 Static lock bytes (NTAG21xF)

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.

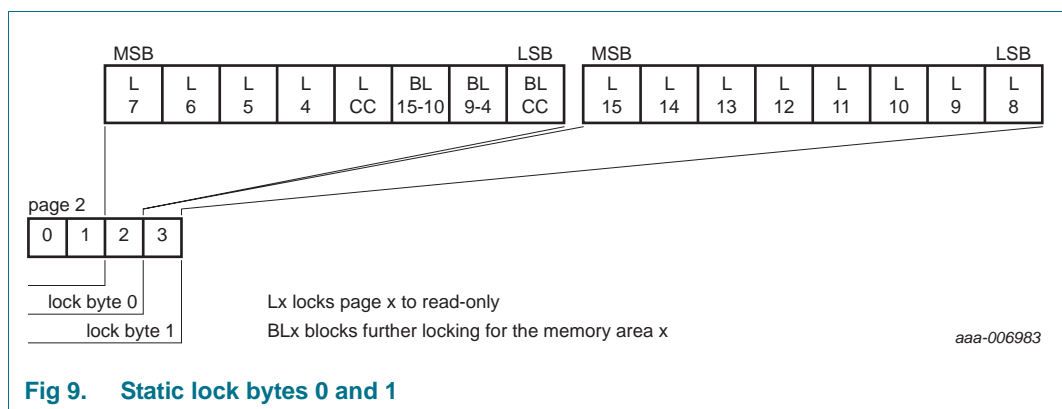


Fig 9. Static lock bytes 0 and 1

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 (NTAG21xF)

To lock the User Memory pages of NTAG21xF 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 NTAG213F and at page E2h for NTAG216F. The three lock bytes cover the memory area of 96 data bytes for NTAG213F and 830 data bytes for NTAG216F. The granularity is 2 pages for NTAG213F and 16 pages for NTAG216F compared to a single page for the first 48 bytes as shown in [Figure 10](#) and [Figure 11](#).

Remark: It is recommended to set all bits marked with RFUI to 0, when writing to the dynamic lock bytes.

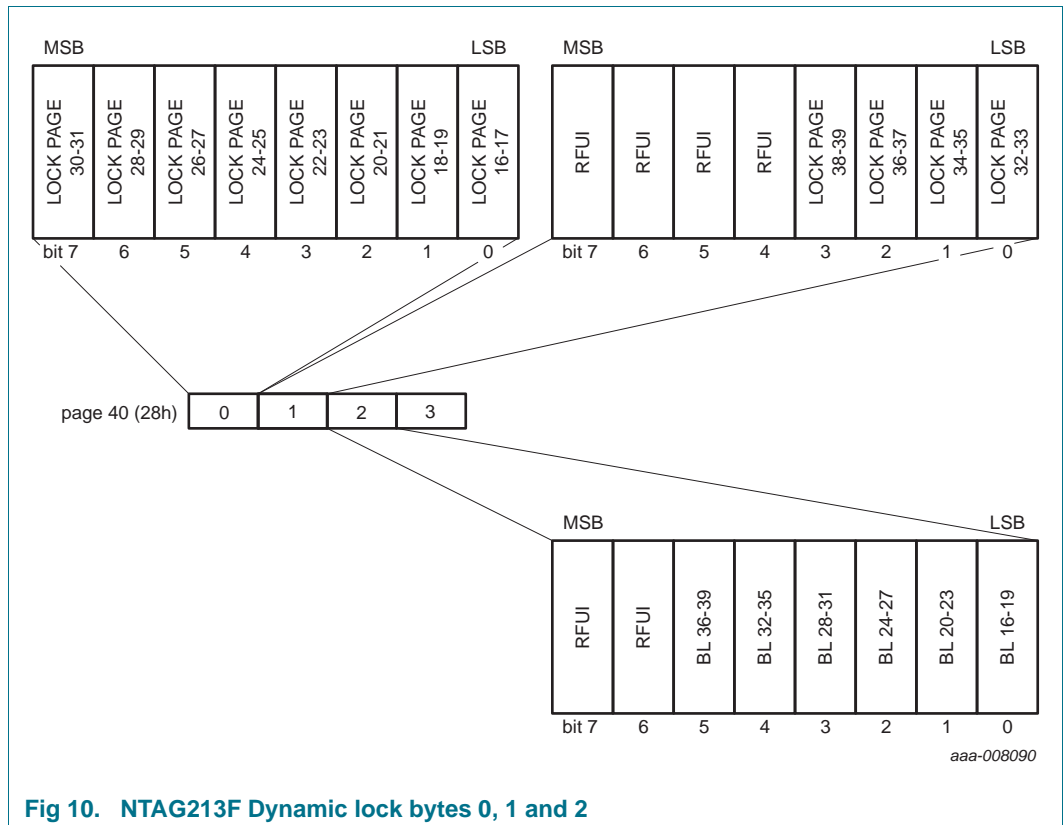


Fig 10. NTAG213F Dynamic lock bytes 0, 1 and 2

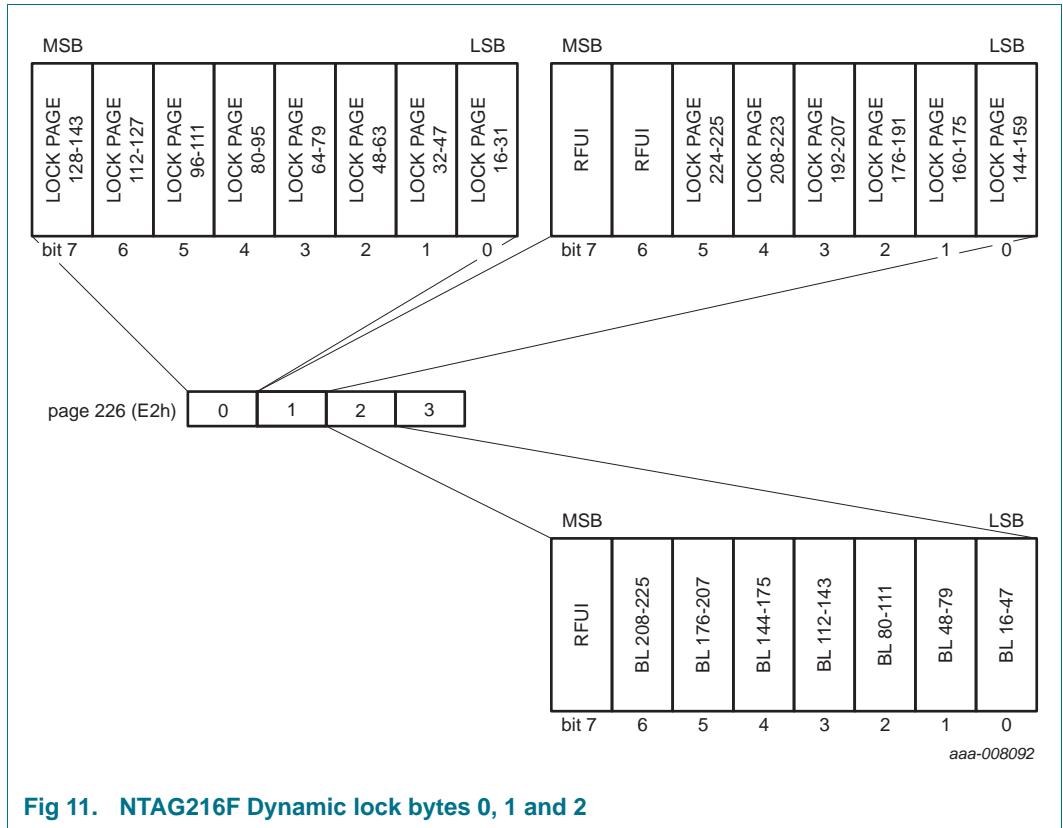


Fig 11. NTAG216F Dynamic lock bytes 0, 1 and 2

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. See example for NTAG213F in [Figure 12](#).

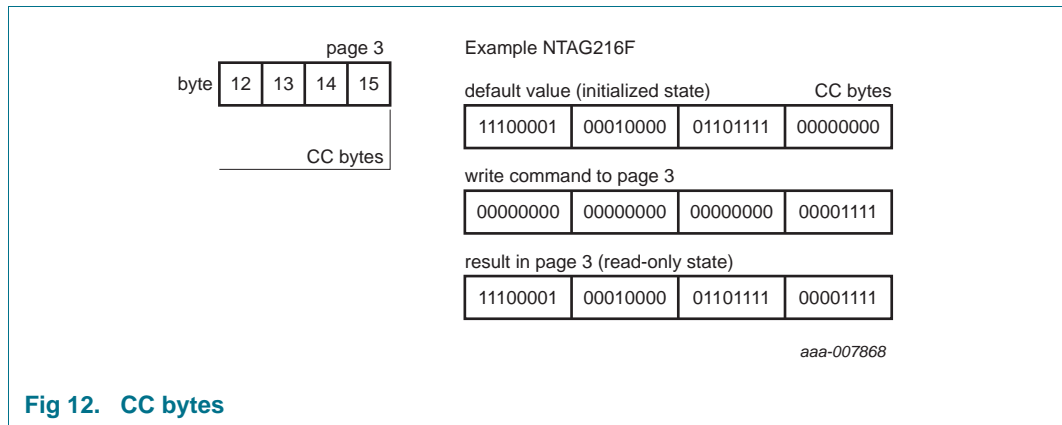


Fig 12. CC bytes

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](#).

To maintain compatibility to NFC Forum Type 2 tag specification (and interoperability with different NFC device), it is recommended to not change the default capability container content.

8.5.5 Data pages

Pages 04h to 27h for NTAG213F and 04h to E1h for NTAG216F 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 8.9](#) 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 NTAG21xF 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 NTAG213F

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 5. Memory content at delivery NTAG216F

Page Address	Byte number within page			
	0	1	2	3
03h	E1h	10h	6Fh	00h
04h	01h	03h	E8h	0Eh
05h	66h	03h	00h	FEh

The access to a part of the user memory area can be restricted using a password verification. Please see [Section 8.9](#) 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 29h to 2Ch for NTAG213F and pages E3h to E6h for NTAG216F variant are used to configure and enable the NTAG 21xF features. 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	29h/E3h	FDP and MIRROR configuration	RFUI	MIRROR_PAGE	AUTH0
17/38	30h/E4h	ACCESS	RFUI	RFUI	RFUI
18/39	31h/E5h	PWD			
19/40	32h/E6h	PACK		RFUI	RFUI

[1] Page address for resp. NTAG213F and NTAG216F

Table 7. FDP and MIRROR configuration

Bit number						
7	6	5	4	3	2	1 0
MIRROR_CONF	MIRROR_Byte		SLEEP_EN	STRG MOD EN	FDP CONF	

Table 8. ACCESS configuration byte

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

Table 9. 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 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)
SLEEP_EN	1	0b	Enables the SLEEP mode function
STRG MOD_EN	1	0b	Controls the tag modulation strength - by default strong modulation is enabled

Table 9. Configuration parameter descriptions

Field	Bit	Default values	Description
FDP CONF	2	11h	FDP CONF defines the configuration of the Field detect pin 00b ... no field detect 01b... enabled by first State-of-Frame (start of communication) 10b... enabled by selection of the tag 11b... enabled by field presence
MIRROR_PAGE	8	00h	MIRROR_Page defines the page for the beginning of the ASCII mirroring A value in the following range enables the ASCII mirror feature 04h-24h ... valid MIRROR_PAGE values for NTAG213F (UID ASCII mirror) 04h-26h ... valid MIRROR_PAGE values for NTAG 213F (NFC counter mirror only) 04h-22h ... valid MIRROR_PAGE values for NTAG213F (both UID and NFC counter mirror) 04h-DEh ... valid MIRROR_PAGE values for NTAG216F (UID ASCII mirror) 04h-E0h ... valid MIRROR_PAGE values for NTAG 216F (NFC counter mirror only) 04h-DCh ... valid MIRROR_PAGE values for NTAG216F (both UID and NFC counter mirror)
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 excluding the PWD and PACK 0b ... user configuration open to write access 1b ... user configuration permanently locked against write access
NFC_CNT_EN	1	0b	Enables the NFC counter 0b ... disabled 1b ... enabled
NFC_CNT_PWD_PROT_EN	1	0b	enables the password protection to read out and mirror the NFC counter 0b ... the protection is disabled 1b ... the protection is enabled
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 NTAG21xF. If write protection is enabled, each write attempt leads to a NAK response.

Remark: Most of the user configuration elements get activated only after the RF reset.

8.6 NFC counter function

NTAG21xF features a NFC counter function. This function enables NTAG21xF to automatically increase the 24 bit counter value, triggered by the first

- READ command or
- FAST-READ command

after the NTAG21xF tag is powered by an RF field.

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 both above listed ways 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

NTAG21xF features a ASCII mirror function. This function enables NTAG21xF 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, NTAG21xF 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 10](#).

Table 10. 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 specified in the range of [Table 9](#).

The MIRROR_CONF bits (see [Table 8](#) and [Table 10](#)) 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).

8.7.1 UID ASCII mirror function

This function enables NTAG21xF 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, NTAG21xF 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, otherwise the mirroring is not executed.

Table 11. Configuration parameter descriptions

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

8.7.1.1 UID ASCII Mirror example

Table 12 show the memory content of a NTAG213F 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 12. UID ASCII mirror - NTAG 213F Physical memory content

Page address		Byte number				ASCII
dec.	hex.	0	1	2	3	
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 13.

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 13. UID ASCII mirror - NTAG 213F Virtual memory content

Page address		Byte number				ASCII
dec.	hex.	0	1	2	3	
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 NTAG21xF 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, NTAG21xF 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 and MIRROR_BYTE value according to [Table 9](#) 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.

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, otherwise the mirroring will not be executed.

Table 14. Configuration parameter descriptions

	MIRROR_PAGE	MIRROR_BYTE bits
Minimum values	04h	00b - 11b
Maximum value	last user memory page - 1	01b

8.7.2.1 NFC counter mirror example

[Table 15](#) show the memory content of a NTAG213F 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 15. NFC counter mirror - NTAG 213F Physical memory content

Page address		Byte number				ASCII
dec.	hex.	0	1	2	3	
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 16](#).

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>

Table 16. NFC counter mirror - NTAG213F Virtual memory content

Page address		Byte number				ASCII
dec.	hex.	0	1	2	3	
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	33	=003
13	0Dh	46	33	31	FE	F31.
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	

8.7.3 UID and NFC counter mirror function

This function enables NTAG21xF to virtually mirror the 7 byte UID and 3byte NFC counter value in ASCII code into the physical memory of the IC separated by 1 byte ("x" character, 78h). The length of the mirror requires 21 bytes to mirror the UID, NFC counter value and the separation byte in ASCII code. On the READ or FAST READ command to the involved user memory pages, NTAG21xF will respond with the virtual memory content of the UID and NFC counter in ASCII code.

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

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

The UID and NFC counter mirror function is enabled with a MIRROR_PAGE and a MIRROR_BYTE value according to [Table 9](#) and the MIRROR_CONF bits are set to 11b.

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.

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 21 bytes of the UID and NFC counter mirror shall not exceed the boundary of the user memory, otherwise the mirroring will not be executed.

Table 17. Configuration parameter descriptions

	MIRROR_PAGE	MIRROR_BYTE bits
Minimum values	04h	00b - 11b
Maximum value	last user memory page - 5	10b

8.7.3.1 UID and NFC counter mirror example

Table 18 show the memory content of a NTAG213F 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=00000000000000x000000

Table 18. UID and NFC counter ASCII mirror - NTAG213F Physical memory content

Page address		Byte number				ASCII
dec.	hex.	0	1	2	3	
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	2F	D1	4.(.
6	06h	01	2B	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	78	000x
16	10h	30	30	30	30	0000
17	11h	30	30	FE	00	00..
18	12h	00	00	00	00
...	...					
39	27h	00	00	00	00
40	28h		dynamic lock bytes		RFUI	
41	29h	D4	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 and 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 19.

Remark: Please note that the separation character “x” (78h) is automatically inserted between the UID mirror and the NFC counter mirror.

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=04E141124C2880x003F31>

Table 19. UID and NFC counter ASCII mirror - NTAG213F Physical memory content

Page address		Byte number				ASCII
dec.	hex.	0	1	2	3	
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	2F	D1	4.(.
6	06h	01	2B	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	78	880x
16	10h	30	30	33	46	003F
17	11h	33	31	FE	00	31..
18	12h	00	00	00	00
...	...					
39	27h	00	00	00	00
40	28h		dynamic lock bytes		RFUI	
41	29h	D4	RFUI	0C	AUTH0	
42	2Ah	Access				
43	2Bh			PWD		
44	2Ch		PACK		RFUI	

8.8 Sleep mode

If the sleep mode is enabled (see configuration bit [Table 9](#)) and the electronic device (e.g. a microcontroller) connected to the NTAG21xF device brings the Field detection pin to GROUND and the NFC device triggers RF reset, then the NTAG21xF device will enter into the sleep mode where it will become invisible for the NFC device (e.g. phone).

This mode is only effective after RF reset, i.e. even if the Field detect pin is brought to ground during HF communication, this will have no impact on the ongoing device activities.

See [Ref. 8](#) for additional information and [Table 41](#) for the voltage range to be applied on the field detection pin for effective sleep mode.

The Field detect pin shall not be left floating.

8.9 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 shall be 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 NTAG21xF, 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 NTAG21xF 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.

8.9.1 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 2Bh for NTAG213F and E5h for NTAG216F.

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, which is the 7-byte UID available on NTAG21xF.

8.9.2 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 NTAG21xF.

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. Independently, 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.

8.9.3 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 and that is at least the first page address of the configuration pages (29h for NTAG 213F or E3h for NTAG 216F).

8.10 Originality signature

NTAG21xF 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.

NTAG21xF digital signature is based on standard Elliptic Curve Cryptography, according to the ECDSA algorithm. The use of a standard algorithm and curve ensures easy software integration of the originality check procedure in an application running on a NFC devices without specific hardware requirements.

Each NTAG21xF UID is signed with a NXP private key and the resulting 32-byte signature is stored in a hidden part of the NTAG21xF 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 not only offline, as well as online way to verify originality of NTAG21xF.

9. Command overview

NTAG21xF activation follows the ISO/IEC 14443 Type A. After NTAG21xF has been selected, it can either be deactivated using the ISO/IEC 14443 HLTA command, or the NTAG21xF commands (e.g. READ or WRITE) can be performed. For more details about the tag activation refer to [Ref. 1](#).

9.1 NTAG21xF command overview

All available commands for NTAG21xF are shown in [Table 20](#).

Table 20. 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
READ_CNT ^[2]	-	-	39h
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 NTAG21xF compared to NTAG203F.

9.2 Timings

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

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 $n=9$ (approximately 87 μ s). 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 13](#). For more details refer to [Ref. 1](#).

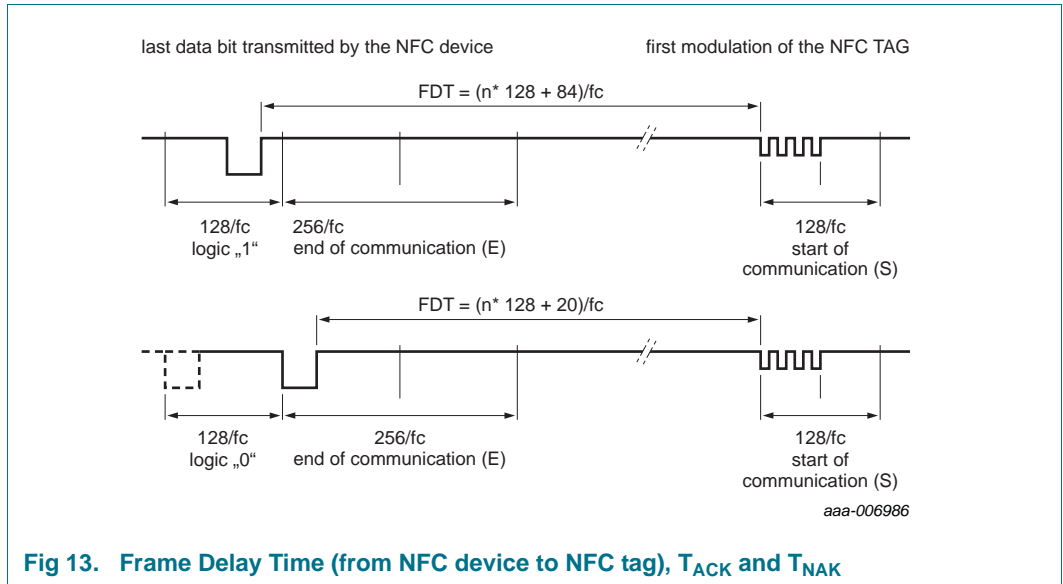


Fig 13. Frame Delay Time (from NFC device to NFC tag), T_{ACK} and T_{NAK}

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 21](#).

Table 21. 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

NTAG21xF replies to a REQA or WUPA command with the ATQA value shown in Table 22. It replies to a Select CL2 command with the SAK value shown in Table 23. The 2-byte ATQA value is transmitted with the least significant byte first (44h).

Table 22. ATQA response of the NTAG21xF

Sales type	Hex value	Bit number															
		16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
NTAG21xF	00 44h	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0

Table 23. SAK response of the NTAG21xF

Sales type	Hex value	Bit number							
		8	7	6	5	4	3	2	1
NTAG21xF	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. NTAG21xF 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 NTAG21xF.

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 NTAG21xF type. The command structure is shown in Figure 14 and Table 24.

Table 25 shows the required timing.

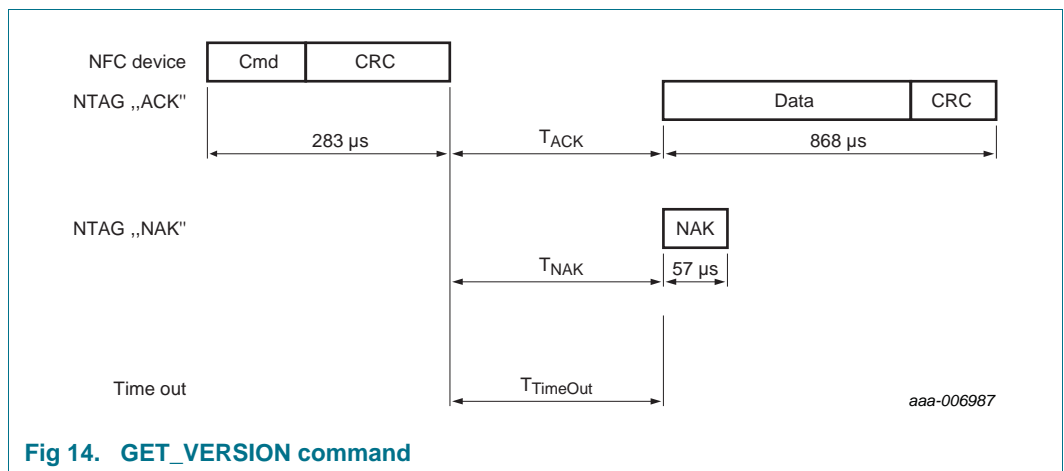


Fig 14. GET_VERSION command

Table 24. 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 21	see Section 9.3	4-bit

Table 25. GET_VERSION timing

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

	T _{ACK/NAK min}	T _{ACK/NAK max}	T _{TimeOut}
GET_VERSION	n=9 ^[1]	T _{TimeOut}	5 ms

[1] Refer to [Section 9.2 "Timings"](#).

Table 26. GET_VERSION response for NTAG213F and NTAG216F

Byte no.	Description	NTAG213F	NTAG216 F	Interpretation
0	fixed Header	00h	00h	
1	vendor ID	04h	04h	NXP Semiconductors
2	product type	04h	04h	NTAG
3	product subtype	01h	01h	50 pF
4	major product version	01h	01h	1
5	minor product version	00h	00h	V0
6	storage size	0Fh	12h	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 NTAG213F is 144 bytes. This memory size is between 128 bytes (2^7) and 256 bytes (2^8). Therefore, the most significant 7 bits of the value 0Fh are interpreted as 7d and the least significant bit is 1b.

The user memory for NTAG216F is 888 bytes. This memory size is between 512 bytes (2^9) and 1024 bytes (2^{10}). Therefore, the most significant 7 bits of the value 12h are interpreted as 9d and the least significant bit is 1b.

10.2 READ

The READ command requires a start page address, and returns the 16 bytes of four NTAG21xF 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 special condition see the end of the paragraph and the roll over mechanism.

The command structure is shown in [Figure 15](#) and [Table 27](#).

[Table 28](#) shows the required timing.

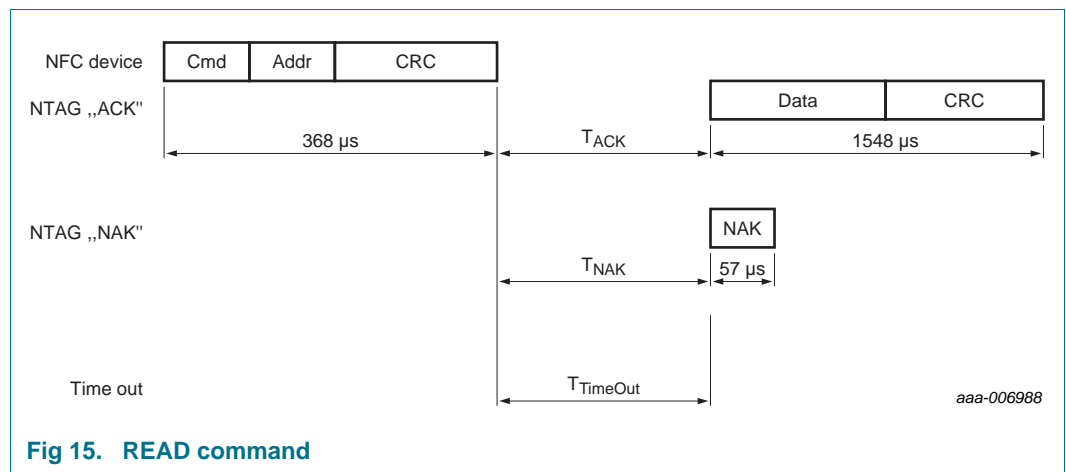


Fig 15. READ command

Table 27. 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 21	see Section 9.3	4-bit

Table 28. READ timing

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

	T _{ACK/NAK} min	T _{ACK/NAK} max	T _{TimeOut}
READ	n=9 ^[1]	T _{TimeOut}	5 ms

[1] Refer to [Section 9.2 "Timings"](#).

In the initial state of NTAG21xF, all memory pages are allowed as Addr parameter to the READ command.

- page address 00h to 2Ch for NTAG213F
- page address 00h to E6h for NTAG216F

Addressing a memory page beyond the limits above results in a NAK response from NTAG21xF.

A roll-over mechanism is implemented to continue reading from page 00h once the end of the accessible memory is reached. Reading from address 2Ah on a NTAG213F results in pages 2Ah, 2Bh, 2Ch and 00h being returned.

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

- if NTAG21xF 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 NTAG21xF is in the AUTHENTICATED state
 - the READ command behaves like on a NTAG21xF 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, NTAG21xF replies a NAK.

For details on the command structure, refer to [Figure 16](#) and [Table 29](#).

[Table 30](#) shows the required timing.

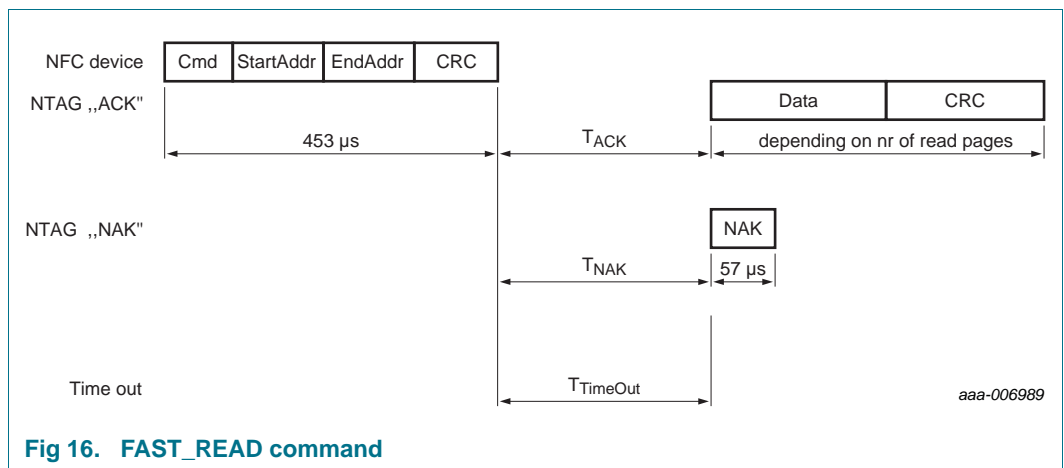


Fig 16. FAST_READ command

Table 29. 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 21	see Section 9.3	4-bit

Table 30. FAST_READ timing

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

	T _{ACK/NAK} min	T _{ACK/NAK} max	T _{TimeOut}
FAST_READ	n=9 ^[1]	T _{TimeOut}	5 ms

[1] Refer to [Section 9.2 "Timings"](#).

In the initial state of NTAG21xF, all memory pages are allowed as StartAddr parameter to the FAST_READ command.

- page address 00h to 2Ch for NTAG213F
- page address 00h to E6h for NTAG216F

Addressing a memory page beyond the limits above results in a NAK response from NTAG21xF.

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 NTAG21xF is in the ACTIVE state
 - if any requested page address is equal or higher than AUTH0 a NAK is replied
- if NTAG21xF is in the AUTHENTICATED state
 - the FAST_READ command behaves like on a NTAG21xF 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 NTAG21xF page. The WRITE command is shown in [Figure 17](#) and [Table 31](#).

[Table 32](#) shows the required timing.

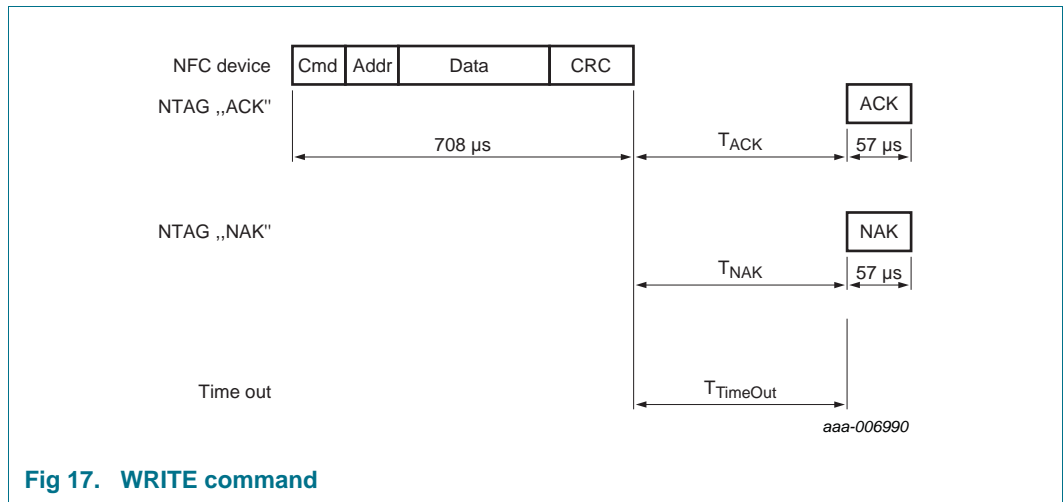


Fig 17. WRITE command

Table 31. 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 21	see Section 9.3	4-bit

Table 32. WRITE timing

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

	T _{ACK/NAK} min	T _{ACK/NAK} max	T _{TimeOut}
WRITE	n=9 ^[1]	T _{TimeOut}	10 ms

[1] Refer to [Section 9.2 "Timings"](#).

In the initial state of NTAG21xF, the following memory pages are valid Addr parameters to the WRITE command.

- page address 02h to 2Ch for NTAG213F
- page address 02h to E6h for NTAG216F

Addressing a memory page beyond the limits above results in a NAK response from NTAG21xF.

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 NTAG21xF is in the ACTIVE state
 - writing to a page which address is equal or higher than AUTH0 results in a NAK response
- if NTAG21xF is in the AUTHENTICATED state
 - the WRITE command behaves like on a NTAG21xF without access protection

NTAG21xF 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 28h containing the additional dynamic lock bits for the NTAG213F
- page E2h containing the additional dynamic lock bits for the NTAG216F

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 NTAG21xF, only the least significant 4 bytes (bytes 0 to 3) are written to the specified address. It is recommended to set all the remaining bytes, 04h to 0Fh, to logic 00h. The COMPATIBILITY_WRITE command is shown in [Figure 18](#), [Figure 19](#) and [Table 31](#).

[Table 34](#) shows the required timing.

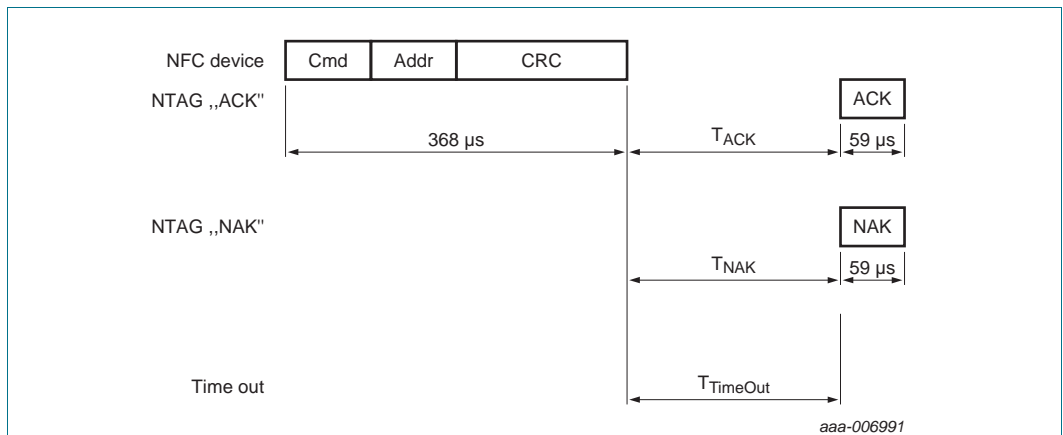


Fig 18. COMPATIBILITY_WRITE command part 1

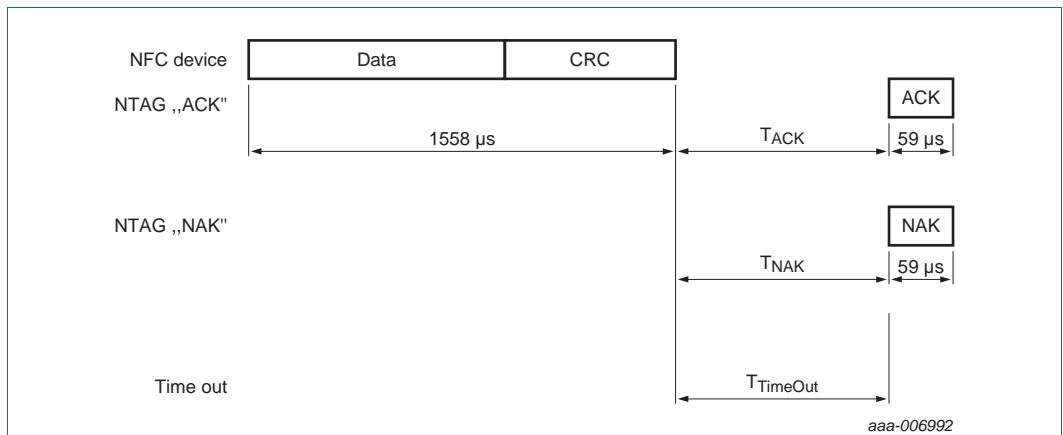


Fig 19. COMPATIBILITY_WRITE command part 2

Table 33. 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 21	see Section 9.3	4-bit

Table 34. COMPATIBILITY_WRITE timing

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

	T _{ACK/NAK min}	T _{ACK/NAK 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 NTAG21xF, the following memory pages are valid Addr parameters to the COMPATIBILITY_WRITE command.

- page address 00h to 2Ch for NTAG213F
- page address 00h to E6h for NTAG216F

Addressing a memory page beyond the limits above results in a NAK response from NTAG21xF.

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 NTAG21xF is in the ACTIVE state
 - writing to a page which address is equal or higher than AUTH0 results in a NAK response
- if NTAG21xF is in the AUTHENTICATED state
 - the COMPATIBILITY_WRITE command behaves the same as on a NTAG21xF without access protection

NTAG21xF 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 28h containing the additional dynamic lock bits for the NTAG213F
- page E2h containing the additional dynamic lock bits for the NTAG216F

10.6 READ_CNT

The READ_CNT command is used to read out the current value of the NFC one-way counter of the NTAG213F, NTAG216F. The command has a single argument specifying the counter number and returns the 24-bit counter value of the corresponding counter. If the NFC_CNT_PWD_PROT bit is set to 1b the counter is password protected and can only be read with the READ_CNT command after a previous valid password authentication (see Section 10.7). The command structure is shown in Figure 20 and Table 35.

Table 36 shows the required timing.

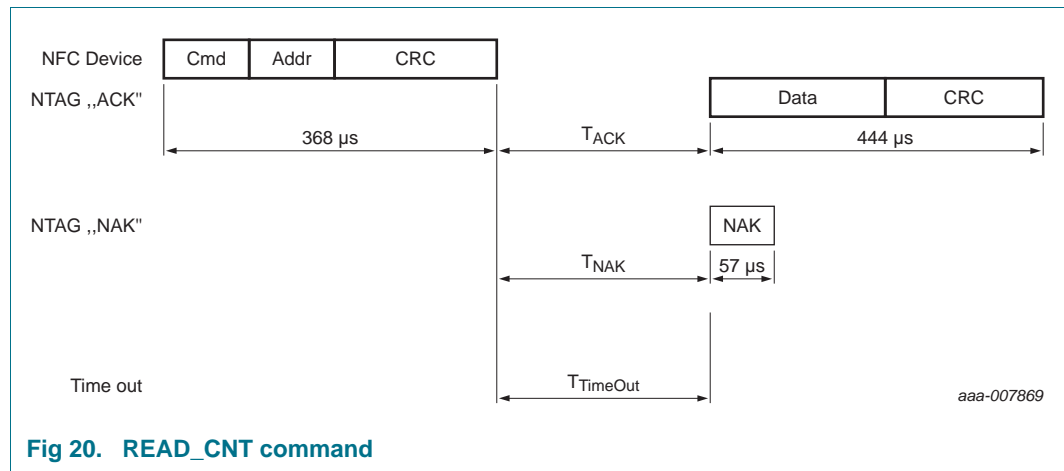


Fig 20. READ_CNT command

Table 35. READ_CNT command

Name	Code	Description	Length
Cmd	39h	read counter	1 byte
Addr	02h	NFC counter address	1 byte
CRC	-	CRC according to Ref. 1	2 bytes
Data	-	counter value	3 bytes
NAK	see Table 21	see Section 9.3	4-bit

Table 36. READ_CNT timing

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

	T _{ACK/NAK min}	T _{ACK/NAK max}	T _{TimeOut}
READ_CNT	n=9 ^[1]	T _{TimeOut}	5 ms

[1] Refer to Section 9.2 "Timings".

The following conditions apply if the NFC counter is password protected:

- if NTAG21xF is in the ACTIVE state
 - Response to the READ_CNT command results in a NAK response
- if NTAG21xF is in the AUTHENTICATED state
 - Response to the READ_CNT command is the current counter value plus CRC

10.7 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 21](#) and [Table 37](#).

[Table 38](#) shows the required timing.

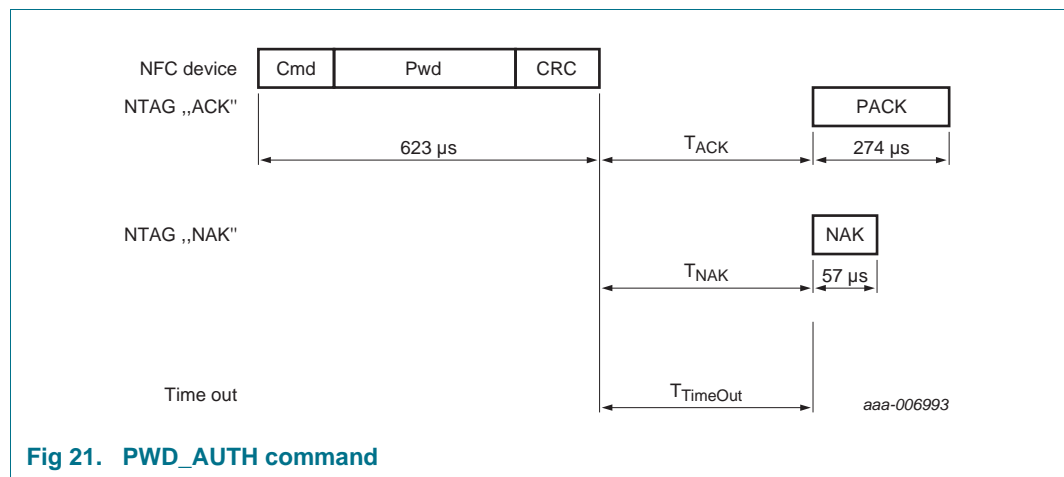


Fig 21. PWD_AUTH command

Table 37. 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 21	see Section 9.3	4-bit

Table 38. PWD_AUTH timing

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

	T _{ACK/NAK} min	T _{ACK/NAK} 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.

10.8 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 22](#) and [Table 39](#).

[Table 40](#) shows the required timing.

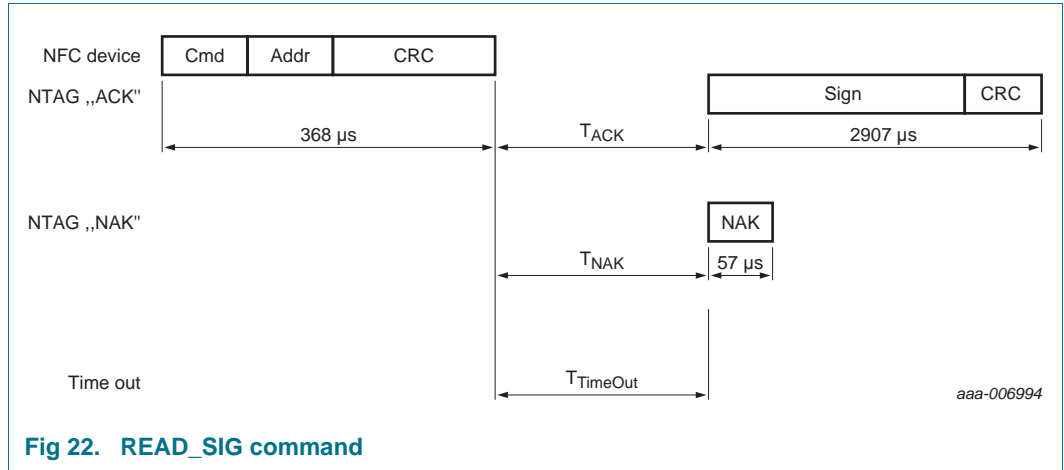


Fig 22. READ_SIG command

Table 39. 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 21	see Section 9.3	4 bit

Table 40. READ_SIG timing

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

	T _{ACK/NAK} min	T _{ACK/NAK} 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 NTAG21xF.

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 41. 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
$V_{FD\ pin}$	Voltage on the Field Detection pin	-0,5	4,6	V
T_{stg}	storage temperature	-55	125	°C
V_{ESD}	electrostatic discharge voltage for all pads	[1] 2	-	kV

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

12. Characteristics

Table 42. Characteristics

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
C_i	input capacitance		-	50.0	-	pF
f_i	input frequency		-	13.56	-	MHz
T_{amb}	ambient temperature		-25		70	°C
$V_{IL, FDpin}$	LOW-level input voltage on FD-pin for sleep mode detection		-0,3	0	0,7	V
$V_{IH, FDpin}$	HIGH-level input voltage on FD-pin for sleep mode detection		1,2		3,6	V
$V_{OL, FD\ pin}$	LOW-level out put voltage on FD-pin	$I_o = 50\mu A$		0	0,05	V
		$I_o = 4mA$		0,35	0,5	V
		$I_o = 8mA$		0,8	1,2	V
EEPROM characteristics						
t_{ret}	retention time	$T_{amb} = 22\ ^\circ C$	10	-	-	year
$N_{endu(W)}$	write endurance	$T_{amb} = 22\ ^\circ C$	100.000	-	-	cycle

13. Package outline

HXSON4: plastic thermal enhanced extremely thin small outline package; no leads;
4 terminals; body 2.0 x 1.5 x 0.5 mm

SOT1312-1

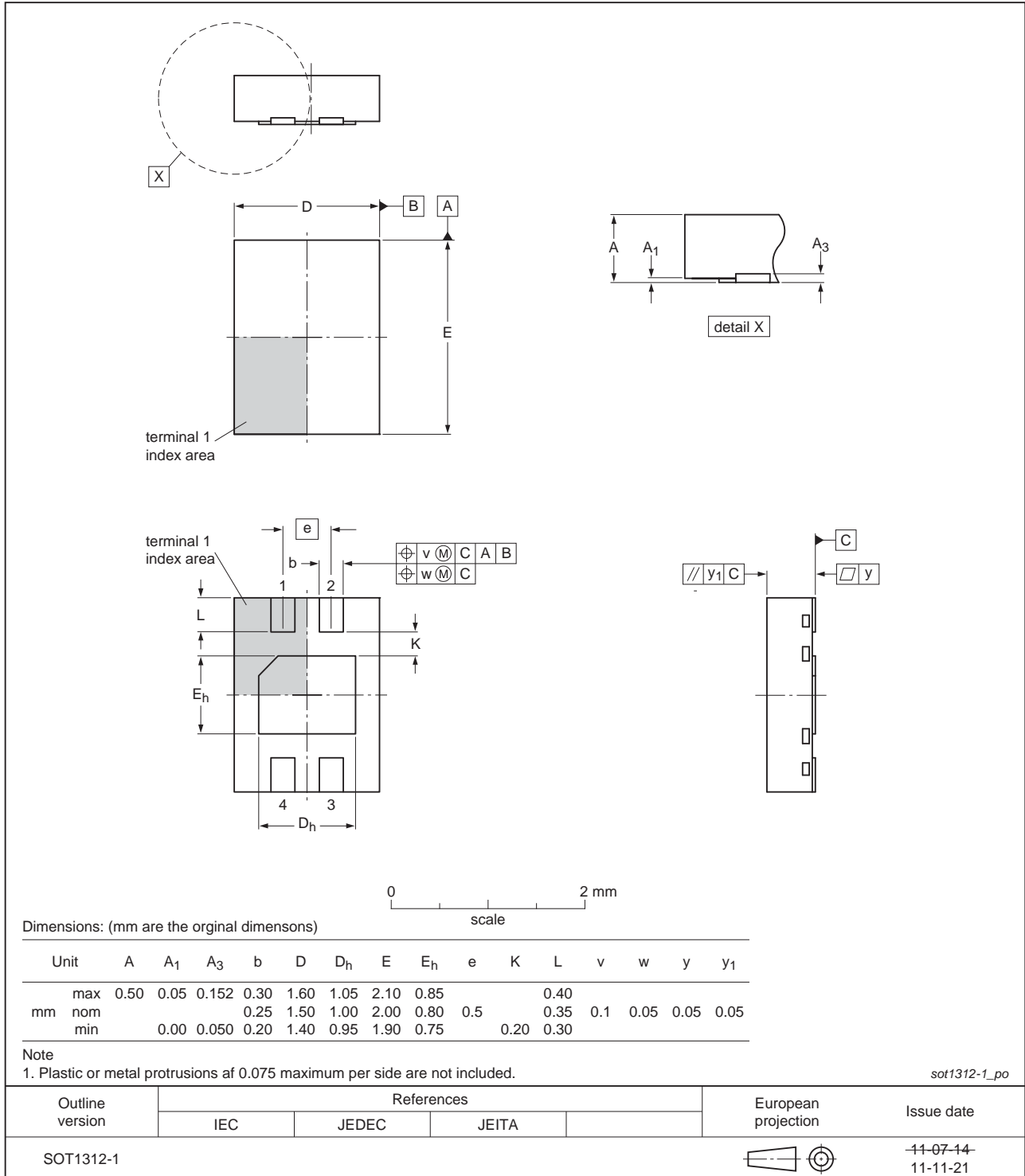


Fig 23. Package outline SOT1312AB2 (HXSON4)

14. Abbreviations

Table 43. 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
LSB	Least Significant Bit
NAK	Not AcKnowledge
NFC device	NFC Forum device
NFC tag	NFC Forum tag
REQA	REQuest command, Type A
RF	Radio Frequency
RFUI	Reserver for Future Use - Implemented
RMS	Root Mean Square
SAK	Select AcKnowledge, type A
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
- [8] **AN11383 NTAG21xF, Field detection and sleep mode feature** — Application note, BU-ID Document number 2709**

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

16. Revision history

Table 44. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
NTAG213F_216F v.3.0	20130718	Product data sheet	-	NTAG213F_216F v.2.3
Modifications:	• General update			
NTAG213F_216F v.2.3	20130606	Preliminary data sheet	-	-

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

Table 1.	Ordering information	5	Table 21.	ACK and NAK values.	33
Table 2.	Pin description of the HXSON4 package	6	Table 22.	ATQA response of the NTAG21xF	34
Table 3.	Marking HXSON4	6	Table 23.	SAK response of the NTAG21xF	34
Table 4.	Memory content at delivery NTAG213F	17	Table 24.	GET_VERSION command	35
Table 5.	Memory content at delivery NTAG216F	17	Table 25.	GET_VERSION timing	35
Table 6.	Configuration Pages	18	Table 26.	GET_VERSION response for NTAG213F and NTAG216F	36
Table 7.	FDP and MIRROR configuration	18	Table 27.	READ command	37
Table 8.	ACCESS configuration byte	18	Table 28.	READ timing	37
Table 9.	Configuration parameter descriptions	18	Table 29.	FAST_READ command	39
Table 10.	Required memory space for ASCII mirror	20	Table 30.	FAST_READ timing	39
Table 11.	Configuration parameter descriptions	21	Table 31.	WRITE command	41
Table 12.	UID ASCII mirror - NTAG 213F Physical memory content	22	Table 32.	WRITE timing	41
Table 13.	UID ASCII mirror - NTAG 213F Virtual memory content	23	Table 33.	COMPATIBILITY_WRITE command	43
Table 14.	Configuration parameter descriptions	24	Table 34.	COMPATIBILITY_WRITE timing	44
Table 15.	NFC counter mirror - NTAG 213F Physical memory content	25	Table 35.	READ_CNT command	45
Table 16.	NFC counter mirror - NTAG213F Virtual memory content	26	Table 36.	READ_CNT timing	45
Table 17.	Configuration parameter descriptions	27	Table 37.	PWD_AUTH command	46
Table 18.	UID and NFC counter ASCII mirror - NTAG213F Physical memory content	28	Table 38.	PWD_AUTH timing	46
Table 19.	UID and NFC counter ASCII mirror - NTAG213F Physical memory content	29	Table 39.	READ_SIG command	47
Table 20.	Command overview	32	Table 40.	READ_SIG timing	47
			Table 41.	Limiting values	48
			Table 42.	Characteristics	48
			Table 43.	Abbreviations and symbols	50
			Table 44.	Revision history	52

20. Figures

Fig 1.	Contactless system	1
Fig 2.	Field detection implementation in NTAG21xF	2
Fig 3.	Block diagram of NTAG213F/216F	5
Fig 4.	Pin configuration for SOT1312AB2 (HXSON4)	6
Fig 5.	State diagram	9
Fig 6.	Memory organization NTAG213F	12
Fig 7.	Memory organization NTAG216F	12
Fig 8.	UID/serial number	13
Fig 9.	Static lock bytes 0 and 1	13
Fig 10.	NTAG213F Dynamic lock bytes 0, 1 and 2	14
Fig 11.	NTAG216F Dynamic lock bytes 0, 1 and 2	15
Fig 12.	CC bytes	16
Fig 13.	Frame Delay Time (from NFC device to NFC tag), T_{ACK} and T_{NAK}	33
Fig 14.	GET_VERSION command	34
Fig 15.	READ command	37
Fig 16.	FAST_READ command	39
Fig 17.	WRITE command	41
Fig 18.	COMPATIBILITY_WRITE command part 1	43
Fig 19.	COMPATIBILITY_WRITE command part 2	43
Fig 20.	READ_CNT command	45
Fig 21.	PWD_AUTH command	46
Fig 22.	READ_SIG command	47
Fig 23.	Package outline SOT1312AB2 (HXSON4)	49

21. Contents

1	General description	1	8.9.1	Programming of PWD and PACK.	30
1.1	Contactless energy and data transfer.	1	8.9.2	Limiting negative verification attempts.	31
1.2	Simple deployment and user convenience.	2	8.9.3	Protection of special memory segments	31
1.3	Security.	2	8.10	Originality signature.	31
1.4	Field detection	2	9	Command overview	32
1.5	Sleep mode	3	9.1	NTAG21xF command overview	32
1.6	NFC Forum Tag 2 Type compliance.	3	9.2	Timings.	32
1.7	Anticollision.	3	9.3	NTAG ACK and NAK	33
2	Features and benefits	4	9.4	ATQA and SAK responses.	34
2.1	EEPROM	4	10	NTAG21xF commands	34
3	Applications	4	10.1	GET_VERSION	34
4	Ordering information	5	10.2	READ	37
5	Block diagram	5	10.3	FAST_READ	39
6	Pinning information	6	10.4	WRITE	41
6.1	Pinning	6	10.5	COMPATIBILITY_WRITE.	43
7	Marking	6	10.6	READ_CNT	45
7.1	Marking HXSON4	6	10.7	PWD_AUTH.	46
8	Functional description	7	10.8	READ_SIG.	47
8.1	Block description	7	11	Limiting values	48
8.2	RF interface	8	12	Characteristics	48
8.3	Data integrity.	8	13	Package outline	49
8.4	Communication principle	9	14	Abbreviations	50
8.4.1	IDLE state.	10	15	References	51
8.4.2	READY1 state.	10	16	Revision history	52
8.4.3	READY2 state.	10	17	Legal information	53
8.4.4	ACTIVE state	11	17.1	Data sheet status	53
8.4.5	AUTHENTICATED state	11	17.2	Definitions	53
8.4.6	HALT state	11	17.3	Disclaimers	53
8.5	Memory organization	12	17.4	Licenses	54
8.5.1	UID/serial number.	13	17.5	Trademarks	54
8.5.2	Static lock bytes (NTAG21xF).	13	18	Contact information	54
8.5.3	Dynamic Lock Bytes (NTAG21xF)	14	19	Tables	55
8.5.4	Capability Container (CC bytes).	16	20	Figures	55
8.5.5	Data pages	16	21	Contents	56
8.5.6	Memory content at delivery	17			
8.5.7	Configuration pages	18			
8.6	NFC counter function	20			
8.7	ASCII mirror function	20			
8.7.1	UID ASCII mirror function	21			
8.7.1.1	UID ASCII Mirror example	22			
8.7.2	NFC counter mirror function	23			
8.7.2.1	NFC counter mirror example	25			
8.7.3	UID and NFC counter mirror function.	26			
8.7.3.1	UID and NFC counter mirror example	28			
8.8	Sleep mode	29			
8.9	Password verification protection.	30			

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

© NXP B.V. 2013.

All rights reserved.

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

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

Date of release: 18 July 2013
262230