NT2H1311TT

NTAG 213 TT - NFC T2T compliant IC with Tag Tamper feature

Rev. 1.1 — 28 March 2017
398311

Objective data sheet
COMPANY PUBLIC

1. General description

NTAG 213 TT offers extended features compared to the NTAG 213 providing additional benefits for smart packaging and brand protection. NTAG 213 TT the new tag tamper functionality which is detecting the status of a tag tamper wire during the startup. In case of an open detection wire, the NTAG 213 TT permanently stores this event. Information status of the tag tamper wire can be mirrored in ASCII code into the user memory which contains the NDEF message or can be read with a dedicated command

Further on the NTAG 213 TToffers the improved originality signature which can be programmed and locked during the tag initialization

The NTAG 213 TT is fully compliant to NFC Forum Type 2 Tag (Ref. 2) and ISO/IEC14443 Type A (Ref. 1) specifications.

1.1 Contactless energy and data transfer

Communication to NTAG 213 TT 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 NTAG 213 TT 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.

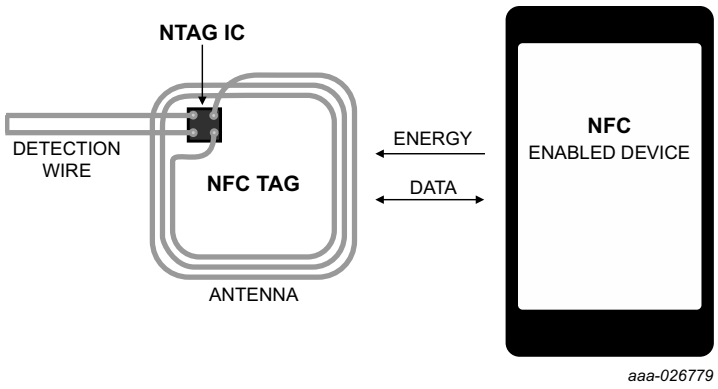


Fig 1. Contactless NTAG 213 TT system

1.2 Simple deployment and user convenience

NTAG 213 TT offers specific features designed to improve integration and user convenience:

- The fast read capability allows scanning 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

1.3 Security

- Manufacturer programmed 7-byte UID for each device
- Pre-programmed Capability container with one time programmable bits
- Field programmable read-only locking function
- Pre-programmed ECC-based originality signature, offering the possibility for customizing and permanently locking
- 32-bit password protection to prevent unauthorized memory operations
- Customer programmed Tag Tamper message which is masked until a tamper event has been detected after startup

1.4 NFC Forum Tag 2 Type compliance

NTAG 213 TT 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 operating more than one tag in the field simultaneously. The anticollision algorithm selects each tag individually. It 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 of NDEF messages
- Automatic NFC counter triggered at read command
- NFC counter ASCII mirror for automatic adding the NFC counter value to the NDEF message
- Tag Tamper feature detecting if the tag tamper wire is open after startup

- Tag Tamper message ASCII mirror copying the customized Tag Tamper message into the NDEF message if there is a detected tamper event
- ECC-based originality signature, offering the possibility for customizing and permanently locking
- Fast read command
- True anticollision
- 50 pF input capacitance

2.1 EEPROM

- 184 bytes organized in 46 pages with 4 bytes per page
- 144 bytes freely available user Read/Write area (36 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
- Configurable password protection with optional limit of unsuccessful attempts
- Anti-tearing support for capability container (CC) and lock bits
- Pre-programmed ECC-based originality signature, offering the possibility for customizing and permanently locking
- Tag Tamper message
- Data retention time of 10 years
- Write endurance 100.000 cycles

3. Applications

- Product authentication
- Smart packaging
- Smart advertisement
- Goods and device authentication
- Voucher and coupons
- Bluetooth or Wi-Fi pairing
- Electronic shelf labels

4. Quick reference data

Table 1. Quick reference data

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

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

5. Ordering information

Table 2. Ordering information

Type number	Package		
	Name	Description	Version
NT2H1311TTDUF	FFC Bump	8 inch wafer, 75 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 144 bytes user memory, 50 pF input capacitance	-
NT2H1311TTDUD	FFC Bump	8 inch wafer, 120µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 144 bytes user memory, 50 pF input capacitance	-

6. Block diagram

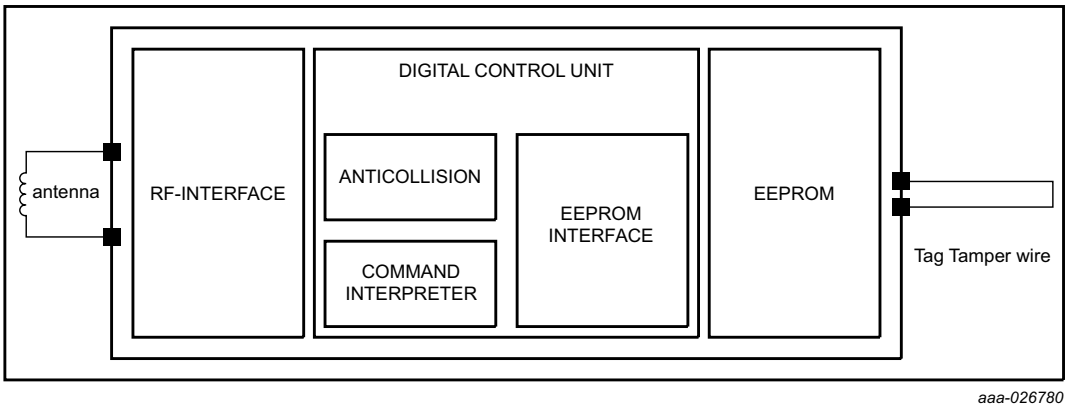


Fig 2. Block diagram of NTAG 213 TT

7. Pinning information

7.1 Pinning

The pinning of the NTAG 213 TT wafer delivery is shown in section “Bare die outline” (see Section 14).

Table 3. Pin allocation table

Pin	Symbol	
LA	LA	Antenna connection LA
LB	LB	Antenna connection LB
DP	DP	Detection Pin
GND	GND	Ground

8. Functional description

8.1 Block description

NTAG 213 TT ICs consist of a 184 bytes 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 NTAG 213 TT. 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 NTAG 213 TT
- EEPROM interface
- NTAG 213 TT EEPROM: 184 bytes, organized in 45 pages of 4 bytes 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

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.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 an 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 has 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. It is then followed by bytes 1 to byte 3 out of this block. The same sequence continues for the next block and all subsequent blocks.

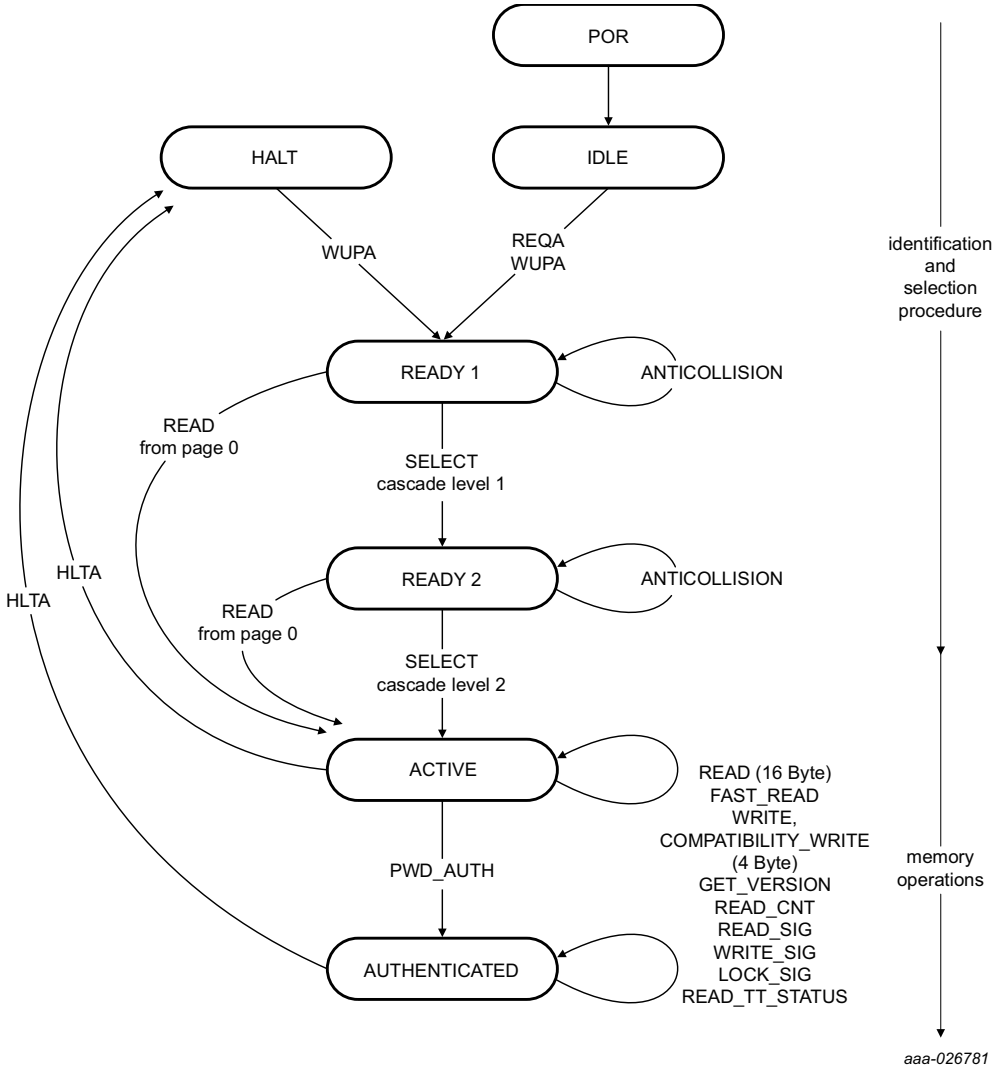
8.3 Data integrity

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 NFC device initiates the commands and the Digital Control Unit of the NTAG 213 TT controls them. 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), NTAG 213 TT 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 NTAG 213 TT 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 NTAG 213 TT into READY2 state where the second part of the UID is resolved.
- READ command (from address 0): all anticollision mechanisms are bypassed and the NTAG 213 TT 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 NTAG 213 TT 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 NTAG 213 TT returns to the IDLE or HALT state.

8.4.3 READY2 state

In this state, NTAG 213 TT 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 NTAG 213 TT 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. NTAG 213 TT is now uniquely selected and only this device communicates with the NFC device even when other contactless devices are present in the NFC device field. If more than one NTAG 213 TT is in the NFC device field, a READ command from address 0 selects all NTAG 213 TT 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 NTAG 213 TT returns to either the IDLE state or HALT state.

8.4.4 ACTIVE state

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

The ACTIVE state is exited with the HLTA command and upon reception NTAG 213 TT 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 NTAG 213 TT returns to either the IDLE state or HALT state.

NTAG 213 TT 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 HALT command and upon reception NTAG 213 TT 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 NTAG 213 TT 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 NTAG 213 TT. An already processed NTAG 213 TT can be set into the HALT state using the HALTA command. In the anticollision phase, this state helps the NFC device to distinguish between processed tags and tags yet to be selected. NTAG 213 TT 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 NTAG 213 TT state remains unchanged.

8.5 Memory organization

The EEPROM memory is organized in pages with 4 bytes per page. NTAG 213 TT has 45 pages in total. The memory organization can be seen in Figure 4, and the functionality of the different memory sections is described in the following sections.

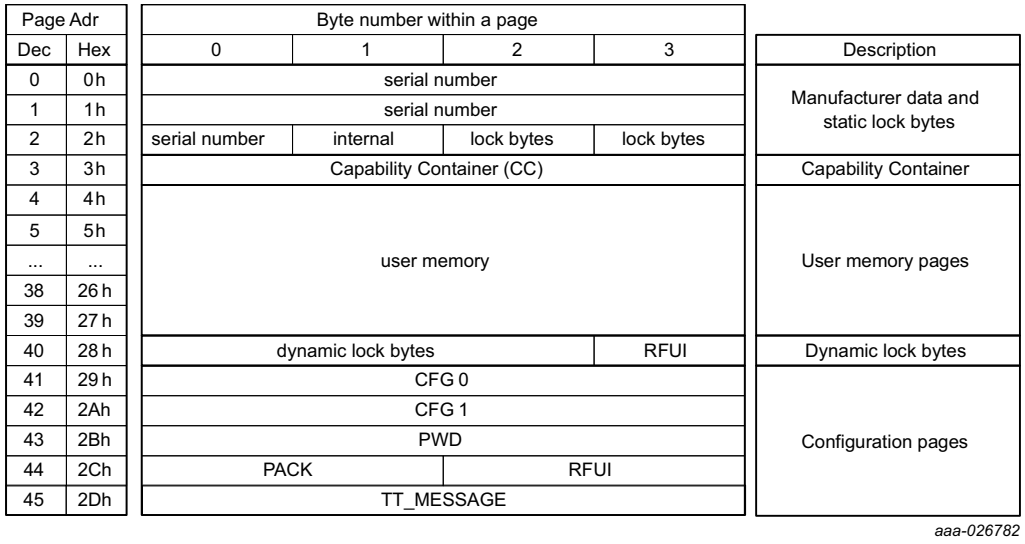


Fig 4. Memory organization NTAG 213 TT

The structure of manufacturing data, lock bytes, capability container and user memory pages are compatible to NTAG 213.

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: It covers 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.

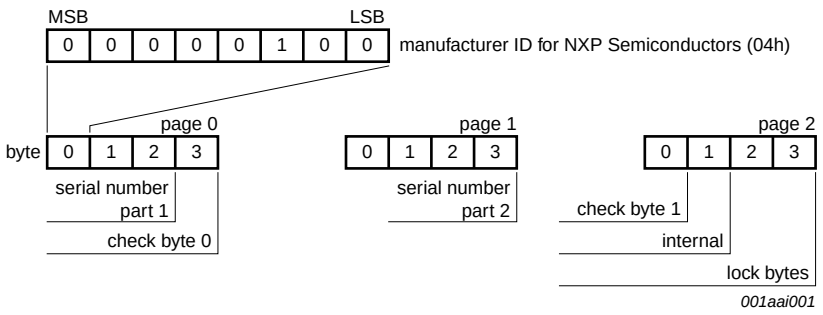


Fig 5. UID/serial number

In accordance with ISO/IEC 14443-3, check byte 0 (BCC0) is defined as CT ⊕ SN0 ⊕ SN1 ⊕ SN2. 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

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.

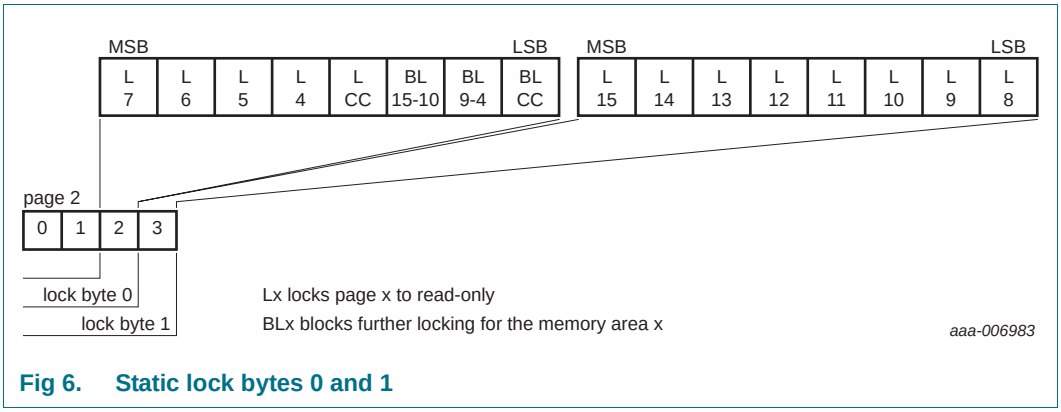


Fig 6. Static lock bytes 0 and 1

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. A WRITE or COMPATIBILITY_WRITE command to block 02h, sets the static locking and block-locking bits. Data bytes 2 and 3 of the WRITE or COMPATIBILITY_WRITE command, and the contents of the lock bytes, are a bit-wise OR. The result becomes the new content of the lock bytes. This process is irreversible. If a bit is set to logic 1, it cannot be changed back to logic 0.

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

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

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

8.5.3 Dynamic Lock Bytes

To lock the pages of NTAG 213 TT starting at page address 10h and onwards, the so called dynamic lock bytes are used. The dynamic lock bytes are at page 28h. The three lock bytes cover the memory area of 96 data bytes. The granularity is 2 pages for NTAG 213 TT (Figure 7).

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

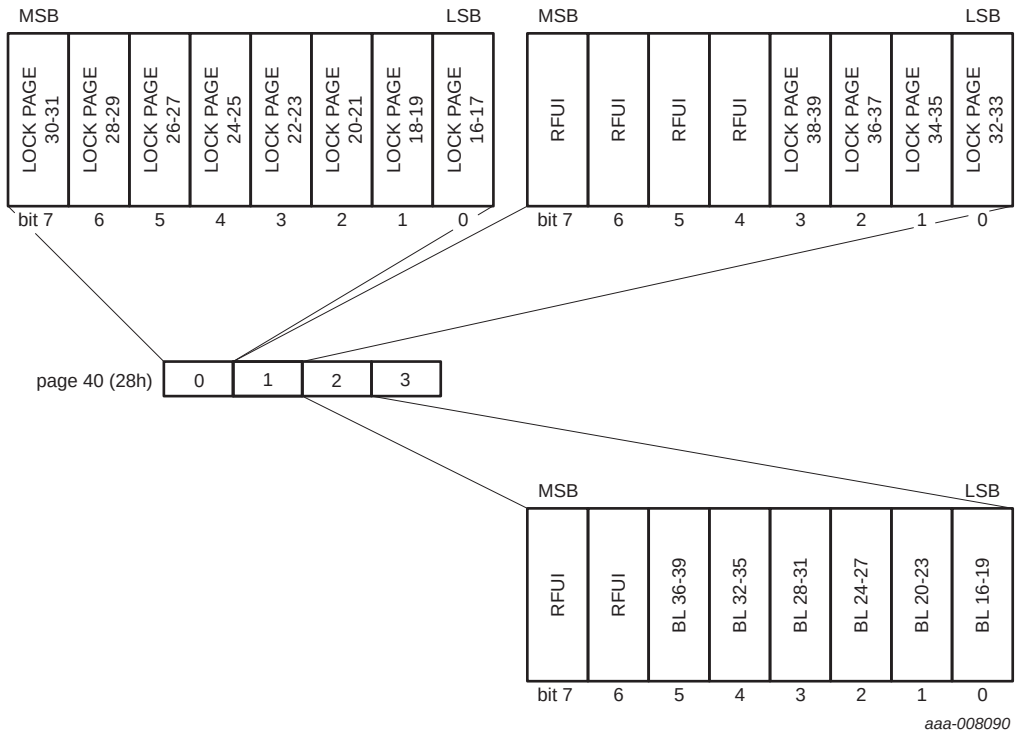


Fig 7. NTAG 213 TT Dynamic lock bytes 0, 1 and 2

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.

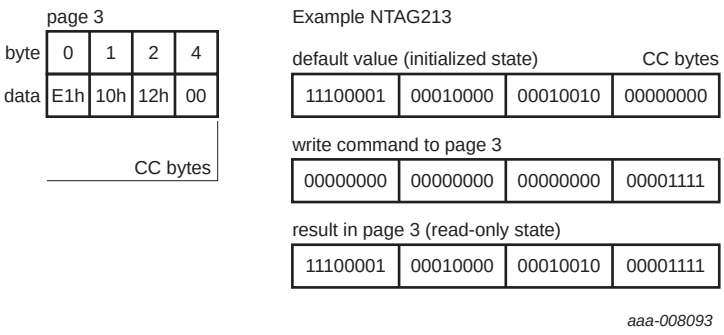


Fig 8. CC bytes example

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

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

Table 4. NDEF memory size

IC	Value in byte 2	NDEF memory size
NTAG 213 TT	12h	144 bytes

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

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

8.5.5 Data pages

Pages 04h to 27h for NTAG 213 TT 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 NTAG 213 TT are pre-programmed as defined in Table 5.

Table 5. Memory content at delivery NTAG 213 TT

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

The access to a part of the user memory area can be restricted using a password verification. 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 2Dh for NTAG 213 TT are used to configure the memory access restriction and to configure the ASCII mirror feature. The memory content of the configuration pages is detailed below.

Table 6. Configuration Pages

Page Address		Byte number			
Dec	Hex	0	1	2	3
41	29h	MIRROR	TT	MIRROR_PAGE	AUTH0
42	2Ah	ACCESS	RFUI	RFUI	RFUI
43	2Bh	PWD			
44	2Ch	PACK		RFUI	RFUI
45	2Dh	TT_MESSAGE			

Table 7. MIRROR configuration byte

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

Table 8. TT (Tag Tamper) configuration byte

Bit number							
7	6	5	4	3	2	1	0
RFUI					TT_LOCK	TT_EN	RFUI

Table 9. ACCESS configuration byte

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

Table 10. Configuration parameter descriptions

Field	Bit	Default values	Description
MIRROR_CONF	3	000b	Defines which mirror shall be used, if the ASCII mirror is enabled by a valid the MIRROR_PAGE byte 000b ... no mirror 001b ... UID ASCII mirror 010b ... NFC counter ASCII mirror 011b ... UID and NFC counter ASCII mirror 100b ... TT (Tag Tamper) ASCII mirror 101b ... UID and TT ASCII mirror 110b ... NFC counter and TT ASCII mirror 111b ... UID, NFC counter and TT ASCII mirror
MIRROR_BYTE	2	00b	The 2 bits define the byte position within the page defined by the MIRROR_PAGE byte (beginning of mirror)
MIRROR_PAGE	8	00h	MIRROR_PAGE defines the page for the beginning of the mirroring A value >03h enables the ASCII mirror feature
TT_LOCK	1	0b	One time programmable bit to lock the Tag Tamper message 0b ... read and write access to the TT_MESSAGE page (2Dh) 1b ... TT_MEESSAGE page 2Dh is locked (irreversible) Once the TT_LOCK bit is set the TT message bytes are masked by 00h on a READ_TT_STATUS command and a READ command to page 2Dh (TT message). Further on the NTAG 213 TT responds with NAK on a WRITE command to page 2Dh (TT message).
TT_EN	1	0b	Tag Tamper feature configuration 0b ... Tag Tamper feature is disabled 1b ... Tag Tamper feature is enabled and TT message is locked (same behavior as TT_Lock bit is set). The NTAG 213 TT performs the Tag Tamper measurement during the startup. If a tag tamper event has been detected, the NTAG 213 TT stores that tag tamper status permanently.
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	1 bit inside the ACCESS byte defining the memory protection 0b ... write access is protected by the password verification 1b ... read and write access is protected by the password verification
CFGLCK	1	0b	Write locking bit for the user configuration 0b ... user configuration open to write access 1b ... user configuration permanently locked against write access, except PWD and PACK
NFC_CNT_EN	1	0b	NFC counter configuration 0b ... NFC counter disabled 1b ... NFC counter enabled If the NFC counter is enabled, the NFC counter will be automatically increased at the first READ or FAST_READ command after a power-on reset

Table 10. Configuration parameter descriptions

Field	Bit	Default values	Description
NFC_CNT_PWD_PROT	1	0b	NFC counter password protection 0b ... NFC counter not protected 1b ... NFC counter password protection enabled If the NFC counter password protection is enabled, the NFC tag will only respond to a READ_CNT command with the NFC counter value after a valid password verification
AUTHLIM	3	000b	Limitation of negative password verification attempts 000b ... limiting of negative password verification attempts disabled 001b-111b ... maximum number of negative password verification attempts
PWD	32	FFFFFFFFh	32-bit password used for memory access protection
PACK	16	0000h	16-bit password acknowledge used during the password verification process
TT_MESSAGE	4	00000000h	Tag tamper message, which is mirrored with the TT ASCII mirror and included in the READ_TT_STATUS response if an open tag tamper wire is detected during startup of the NTAG 213 TT
RFUI	-	not defined	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 NTAG 213 TT. If write protection is enabled, each write attempt leads to a NAK response.

8.6 Tag Tamper feature

NTAG 213 TT features a Tag Tamper function. This function enables NTAG 213 TT to detect at the startup of the IC, if the tag the tag tamper wire is open or closed.

In case of detecting an open tag tamper wire after the NTAG 213 TT tag is powered by an RF field, this event will be permanently stored in the IC.

The 4 byte Tag Tamper message is programmed into TT_MESSAGE page 2Dh by the customer during tag initialization. If the TT_EN or TT_LOCK bit is set to one, the TT_MESSAGE is masked with 4 byte 00h.

The Tag Tamper feature is enabled or disabled with the TT_EN bit (see Section 8.5.7).

The Tag Tamper status can be read with

- READ_TT_STATUS command or
- Tag Tamper ASCII mirror feature

If the tag tamper wire has never been detected as open during startup:

- The READ_TT_STATUS command response is masked with 4 byte 00h
- If the Tag Tamper ASCII mirror is enabled, the original programmed user memory content is read at that position

Once the tag tamper wire has been detected as open during startup:

- NTAG 213 TT stores permanently that the tag tamper wire has been opened

- On a READ_TT_STATUS command, the NTAG 213 TT responses with the programmed TT_MESSAGE form page 2Dh
- If the Tag Tamper ASCII mirror is enabled, the programmed TT_MESSAGE is mirrored in ASCII to the defined position in the user memory (see Section 8.8)

The actual status of the tag tamper wire during startup can be read with the READ_TT_STATUS command (see Section 10.11).

Parameters on the detection for open and closed of the tag tamper wire connected to DP and GND pad are specified in Section 12.

Remark: To avoid interferences induced by the RF field during the measurement of the tag tamper, it is recommended to keep the area covered by the tag tamper wire connected to DP and GND as small as possible. The area may not be larger than 2.5 cm^2 depending on the RF field strength used in the application under worst case conditions.

8.7 NFC counter function

NTAG 213 TT features an NFC counter function. This function enables NTAG 213 TT to automatically increase the 24-bit counter value, triggered by the first valid

- READ command or
- FAST-READ command

after the NTAG 213 TT tag is powered by an RF field.

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

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

The actual NFC counter value can be read with

- READ_CNT command or
- NFC counter mirror feature

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

8.8 ASCII mirror function

NTAG 213 TT features an ASCII mirror function. This function enables NTAG 213 TT to virtually mirror

- 7 byte UID (see Section 8.8.1) or
- 3 byte NFC counter value (see Section 8.8.2) or
- 4 byte Tag Tamper message or
- a combination of the three

into the physical memory of the IC in ASCII code. On the READ or FAST READ command to the involved user memory pages, NTAG 213 TT responds with the virtual memory content of the UID and/or NFC counter value and or Tag Tamper message in ASCII code.

The required length of the reserved physical memory for the mirror functions and the order for the ASCII mirrors is specified in Table 11. If the ASCII mirror exceeds the user memory area, the data will not be mirrored.

Table 11. Required memory space for ASCII mirror

ASCII mirror and order	Required number of bytes in the physical memory
UID mirror	14 bytes
NFC counter mirror	6 bytes
TT message mirror	8 bytes
UID + NFC counter mirror	21 bytes (14 bytes for UID + 1 byte separation + 6 bytes NFC counter value)
UID + TT message mirror	23 bytes (14 bytes for UID + 1 byte separation + 8 bytes TT message)
NFC counter + TT message	15 bytes (6 bytes NFC counter value + 1 byte separation + 8 bytes TT message)
UID + NFC + TT message mirror	30 bytes (14 bytes for UID + 1 byte separation + 6 bytes NFC counter value + 1 byte separation + 8 bytes TT message)

The MIRROR_PAGE and MIRROR_BYTE values defines the position within the user memory where the mirroring of the ASCII mirror.

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

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

The MIRROR_CONF bits (see Table 7 and Table 10) define which ASCII mirrors shall be enabled.

If there is more than one ASCII mirror is enabled, the ASCII mirrors are separated automatically with an “x” character (78h ASCII code).

Remark: Please note that the number of bytes (see Table 11) of the enabled ASCII mirrors shall not exceed the boundary of the user memory. Therefore it is required to use only valid values for MIRROR_BYTE and MIRROR_PAGE to ensure a proper functionality. If the ASCII mirror exceeds the user memory area, the ASCII mirrors does not work properly.

8.8.1 UID ASCII mirror function

This function enables NTAG 213 TT 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, NTAG 213 TT responds with the virtual memory content of the UID in ASCII code.

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

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.

8.8.2 NFC counter mirror function

This function enables NTAG 213 TT 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, NTAG 213 TT responds with the virtual memory content of the NFC counter in ASCII code.

The MIRROR_PAGE and MIRROR_BYTE values define the position within the user memory where the mirroring of the NFC counter shall start depending whether the UID ASCII mirror is enabled or disabled.

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

The NFC counter mirror function is enabled with a MIRROR_PAGE value >03h and the MIRROR_CONF bits.

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 8.7), the NFC_CNT_EN bit shall be set to 1b.

8.8.3 Tag Tamper message mirror function

This function enables NTAG 213 TT to virtually mirror the 4 byte Tag Tamper message in ASCII code into the physical memory of the IC if the tag tamper wire has been once detected as open during startup, when the NTAG 213 TT is powered via the RF field. The Tag Tamper mirror requires 8 bytes to mirror the Tag Tamper message in ASCII code. On the READ or FAST READ command to the involved user memory pages, NTAG 213 TT responds with

- the physical memory of the related part of the user memory, if the tag tamper wire has never been detected as open during startup or
- with the virtual memory content of the Tag Tamper message in ASCII code, which has been programmed into page 2Dh.

The MIRROR_PAGE and MIRROR_BYTE values define the position within the user memory where the mirroring of the Tag Tamper message shall start depending whether the UID and/or NFC counter ASCII mirror is enabled or disabled.

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

The Tag Tamper message mirror function is enabled with a MIRROR_PAGE value >03h and the MIRROR_CONF bits.

Remark: To enable the Tag Tamper feature itself (see Section 8.6), the TT_EN bit shall be set to 1b.

8.8.4 Example for UID, NFC counter and Tag Tamper message ASCII mirror

Table 12 show the memory content of a NTAG 213 TT which has been written to the physical memory. Without the ASCII mirror feature, the content in the programmed 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=00000000000000x000000x00000000

Table 12. UID and NFC counter ASCII mirror - Physical memory content

Page address		Byte number				
dec.	**hex.**	**0**	**1**	**2**	**3**	**ASCII**
0	00h	04	E1	41	2C	
1	01h	12	4C	28	80	
2	02h	F6	internal	lock bytes		
3	03h	E1	10	12	00	
4	04h	01	03	A0	0C	....
5	05h	34	03	38	D1	4.8.
6	06h	01	34	55	01	.4U.
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	78	30	00x0
18	12h	30	30	30	30	0000
19	13h	30	30	30	FE	000.
...	...					
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		
45	2Dh	TT_MESSAGE				

In that example, the following parameters are used

- UID 04 E1 41 12 4C 28 80h

- NFC counter value of e.g. 00 3F 31h
- Tag Tamper message programmed in page 2Dh e.g. A0 23 CD 1Bh

With the related values in the MIRROR_PAGE and the MIRROR_BYTE, the mirroring is starting in page 0Ch byte 1.

If no tag tamper event has been detected during the startup of the NTAG 213 TT only the UID and NFC counter value is mirrored in ACSII code.

The virtual memory content is shown in Table 13.

Remark: Please note that the separation character “x” (78h) is automatically mirrored between the ASCII mirrors.

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

http://www.nxp.com/index.html?m=04E141124C2880x003F31x00000000

Table 13. UID and NFC counter ASCII mirror - Virtual memory content without tag tamper event

Page address		Byte number				
dec.	**hex.**	**0**	**1**	**2**	**3**	**ASCII**
0	00h	04	E1	41	2C	
1	01h	12	4C	28	80	
2	02h	F6	internal	lock bytes		
3	03h	E1	10	12	00	
4	04h	01	03	A0	0C	....
5	05h	34	03	38	D1	4.8.
6	06h	01	34	55	01	.4U.
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	78	30	31x0
18	12h	30	30	30	30	0000
19	13h	30	30	30	FE	000.
...	...					
39	27h	00	00	00	00	....
40	28h	dynamic lock bytes			RFUI	
41	29h	D4	RFUI	0C	AUTH0	
42	2Ah	Access				

Table 13. UID and NFC counter ASCII mirror - Virtual memory content without tag tamper event

Page address		Byte number				
dec.	hex.	0	1	2	3	ASCII
43	2Bh	PWD				
44	2Ch	PACK		RFUI		
45	2Dh	TT_MESSAGE				

Once a tag tamper event has been detected during the startup of the NTAG 213 TT also the programmed Tag Tamper message is mirrored in ASCII code beside the UID and NFC counter value.

The virtual memory content is shown in Table 14.

Remark: Please note that the separation character “x” (78h) is automatically mirrored between the ASCII mirrors.

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

http://www.nxp.com/index.html?m=04E141124C2880x003F31xA023CD1B

Table 14. UID and NFC counter ASCII mirror - Virtual memory content after tag tamper event

Page address		Byte number				
dec.	hex.	0	1	2	3	ASCII
0	00h	04	E1	41	2C	
1	01h	12	4C	28	80	
2	02h	F6	internal	lock bytes		
3	03h	E1	10	12	00	
4	04h	01	03	A0	0C	....
5	05h	34	03	38	D1	4.8.
6	06h	01	34	55	01	.4U.
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	78	41	31xA
18	12h	30	32	33	43	023C
19	13h	44	31	42	FE	D1B.
...	...					
39	27h	00	00	00	00	....

Table 14. UID and NFC counter ASCII mirror - Virtual memory content after tag tamper event

Page address		Byte number				
dec.	**hex.**	**0**	**1**	**2**	**3**	**ASCII**
40	28h	dynamic lock bytes			RFUI	
41	29h	D4	RFUI	0C	AUTH0	
42	2Ah	Access				
43	2Bh	PWD				
44	2Ch	PACK		RFUI		
45	2Dh	TT_MESSAGE				

8.9 Password verification protection

The memory write or read/write access to a configurable part of the memory can be constrained by 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 NTAG 213 TT, password protection is disabled by an 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.

8.9.1 Programming of PWD and PACK

The 32-bit PWD and the 16-bit PACK have 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 recommended to set AUTH0 to the page where the PWD is located after the password has been written. This page is 2Bh for NTAG 213 TT.

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 NTAG 213 TT.

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 NTAG 213 TT.

If AUTHLIM is not equal to 000b, each negative authentication verification is internally counted. The count operation features anti-tearing support. 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.

8.9.3 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.

8.10 Originality signature

The NTAG 213 TT offers a feature to verify the origin of a tag confidently, using the UID toward an originality signature stored in a hidden part of memory. The originality signature can be read with the READ_SIG command.

The NTAG 213 TT provides the possibility to customize the originality signature to personalize the IC individually for specific application.

At delivery, the NTAG 213 TT is pre-programmed with the NXP originality signature described below. This signature is locked in the dedicated memory. If needed, the signature can be unlocked with the LOCK_SIG command. It is reprogrammed with a custom-specific signature using the WRITE_SIG command during the personalization process by the customer. The signature can be permanently locked afterwards with the LOCK_SIG command to avoid further modifications.

Remark: If no customized originality signature is required, it is recommended to lock the NXP signature permanently during the initialization process with the LOCK_SIG command.

8.10.1 Originality Signature at delivery

At the delivery, the NTAG 213 TT is programmed with an NXP digital signature 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 NTAG 213 TT UID is signed with an NXP private key and the resulting 32-byte signature is stored in a hidden part of the NTAG 213 TT memory during IC production.

This signature can be retrieved using the READ_SIG command and 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 are set to secp128r1. It is defined within the standards for elliptic curve cryptography SEC (Ref. 7).

Details on how to check that the NXP signature value is provided in following application note (Ref. 5). It is foreseen to offer an online and offline way to verify originality of NTAG 213 TT.

9. Command overview

NTAG activation follows the ISO/IEC 14443 Type A. After NTAG 213 TT 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 NTAG 213 TT command overview

All available commands for NTAG 213 TT are shown in Table 15.

Table 15. 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	-	-	60h
READ	-	READ	30h
FAST_READ	-	-	3Ah
WRITE	-	WRITE	A2h
COMP_WRITE	-	-	A0h
READ_CNT	-	-	39h
PWD_AUTH	-	-	1Bh
READ_SIG	-	-	3Ch
WRITE_SIG[2]	-	-	A9h
LOCK_SIG[2]	-	-	ACh
READ_TT_STATUS[2]	-	-	A4h

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

[2] This command is new in NTAG 213 TT compared to NTAG 213.

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 transmission times refer to the data frames including start of communication and end of communication. They do not include the encoding (like the Miller pulses). An 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). An 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 timeout 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 command timings are according to ISO/IEC 14443-3 frame specification as shown for the Frame Delay Time in Figure 9. For more details, refer to Ref. 1.

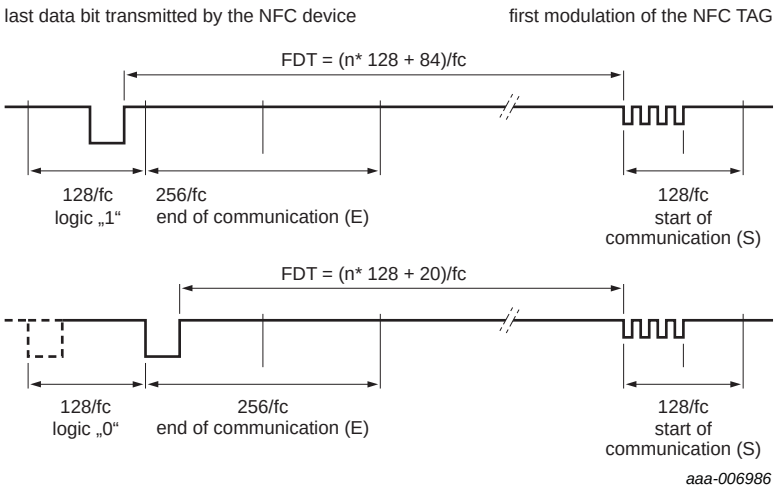


Fig 9. Frame Delay Time (from NFC device to NFC tag)

Remark: Due to the coding of commands, the measured timings usually exclude (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 16.

Table 16. 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
4h	NAK for invalid authentication counter overflow
5h	NAK for EEPROM write error

9.4 ATQA and SAK responses

NTAG 213 TT replies to a REQA or WUPA command with the ATQA value shown in Table 17. It replies to a Select CL2 command with the SAK value shown in Table 18. The 2-byte ATQA value is transmitted with the least significant byte first (44h).

Table 17. ATQA response of the NTAG 213 TT

		Bit number														
Sales type	**Hex value**	**16**	**15**	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
NT2H1311TT	00 44h	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0

Table 18. SAK response of the NTAG 213 TT

		Bit number							
Sales type	**Hex value**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
NT2H1311TT	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 NTAG IC.

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 NTAG IC type. The command structure is shown in Figure 10 and Table 19.

Table 20 shows the required timing.

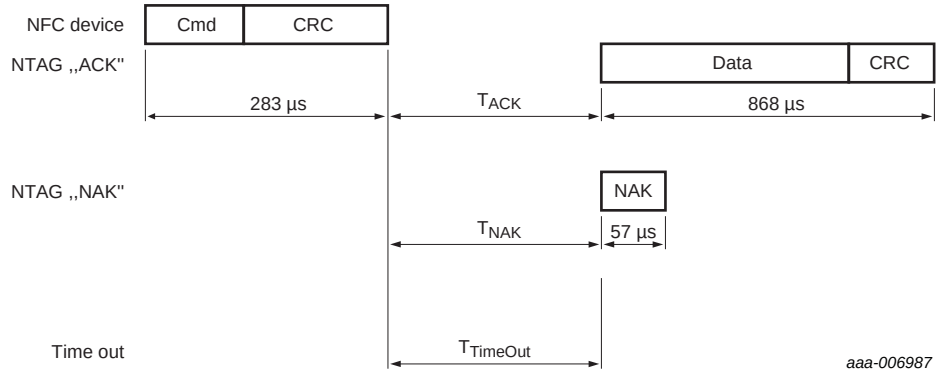


Fig 10. GET_VERSION command

Table 19. 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	8 bytes
NAK	see Table 16	see Section 9.3	4 bits

Table 20. 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 21. GET_VERSION response for NTAG 213 TT

Byte no.	Description	NTAG 213 TT	Interpretation
0	fixed Header	00h	
1	vendor ID	04h	NXP Semiconductors
2	product type	04h	NTAG
3	product subtype	02h	50 pF
4	major product version	03h	3
5	minor product version	00h	V0
6	storage size	0Fh	see following information
7	protocol type	03h	ISO/IEC 14443-3 compliant

The most significant 7 bits of the storage size byte are interpreted as an 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 NTAG 213 TT is 144 bytes. This memory size is between 128 bytes and 256 bytes. Therefore, the most significant 7 bits of the value 0Fh, are interpreted as 7d 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 NTAG 213 TT 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 22.

Table 23 shows the required timing.

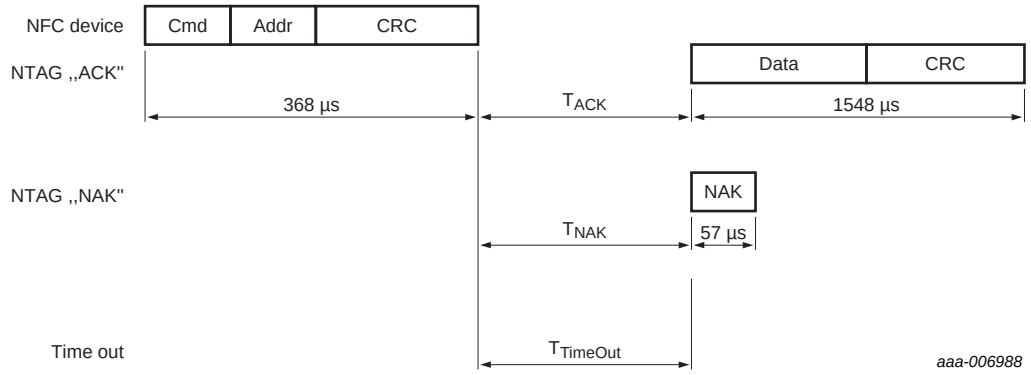


Fig 11. READ command

Table 22. 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 16	see Section 9.3	4 bits

Table 23. 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 NTAG 213 TT, all memory pages are allowed as Addr parameter to the READ command.

- page address 00h to 2Dh for NTAG 213 TT

Addressing a memory page beyond the limits above results in a NAK response from NTAG 213 TT.

A roll-over mechanism is implemented to continue reading from page 00h once the end of the accessible memory is reached. Reading from address 2Bh on a NTAG 213 TT results in pages 2Bh, 2Ch, 2Dh and 00h being returned.

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

- if NTAG 213 TT 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 NTAG 213 TT is in the AUTHENTICATED state
  - the READ command behaves like on a NTAG 213 TT 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 the accessible area, NTAG 213 TT replies a NAK. For details on those cases and the command structure, refer to Figure 12 and Table 24.

Table 25 shows the required timing.

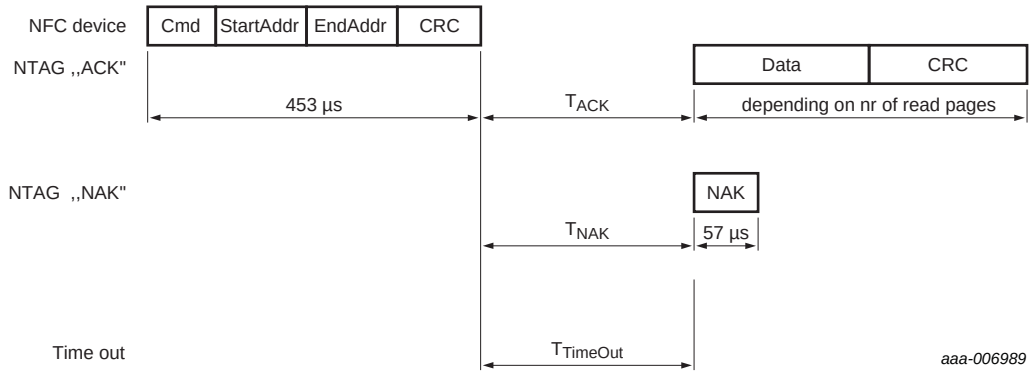


Fig 12. FAST_READ command

Table 24. 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 16	see Section 9.3	4 bits

Table 25. 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 NTAG 213 TT, all memory pages are allowed as StartAddr parameter to the FAST_READ command.

- page address 00h to 2Dh for NTAG 213 TT

Addressing a memory page beyond the limits above results in a NAK response from NTAG 213 TT.

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 NTAG 213 TT is in the ACTIVE state
  - if any requested page address is equal or higher than AUTH0 a NAK is replied
- if NTAG 213 TT is in the AUTHENTICATED state
  - the FAST_READ command behaves like on a NTAG 213 TT 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 NTAG 213 TT page. The WRITE command is shown in Figure 13 and Table 26.

Table 27 shows the required timing.

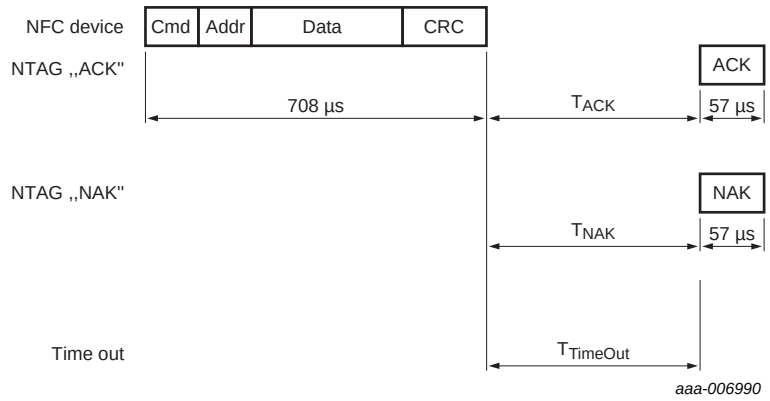


Fig 13. WRITE command

Table 26. 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 16	see Section 9.3	4 bits

Table 27. 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 NTAG 213 TT, the following memory pages are valid Addr parameters to the WRITE command.

- page address 02h to 2Dh for NTAG 213 TT

Addressing a memory page beyond the limits above results in a NAK response from NTAG 213 TT.

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 NTAG 213 TT is in the ACTIVE state
  - writing to a page which address is equal or higher than AUTH0 results in a NAK response
- if NTAG 213 TT is in the AUTHENTICATED state
  - the WRITE command behaves like on a NTAG 213 TT without access protection

Writing to page 2Dh results in NAK if the TT_LOCK and/or TT_EN bits are set to 1.

NTAG 213 TT features tearing protected write operations to specific memory content. The following pages are protected against tearing events during a WRITE operation:

- page 02h containing static lock bits
- page 03h containing CC bits
- page 28h containing the additional dynamic lock bits for the NTAG 213 TT

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 NTAG 213 TT, 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 14, Figure 15 and Table 28.

Table 29 shows the required timing.

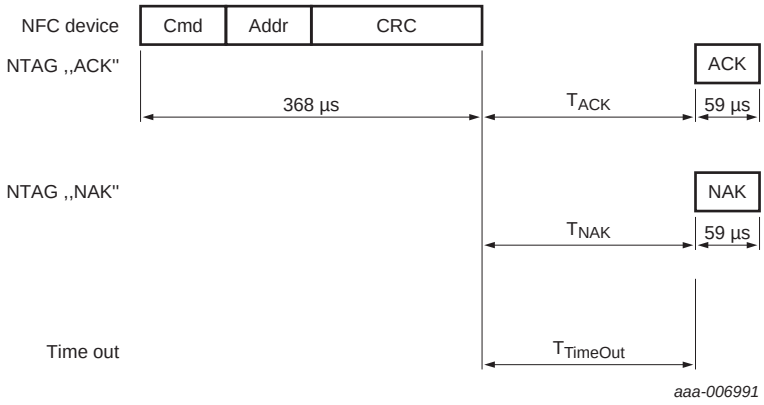


Fig 14. COMPATIBILITY_WRITE command part 1

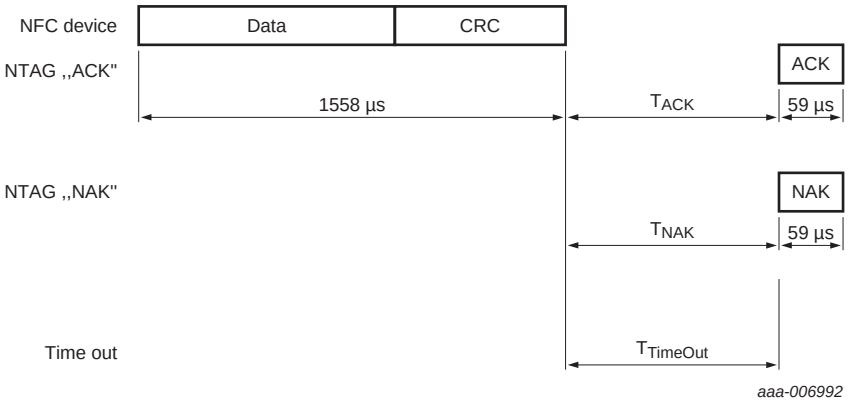


Fig 15. COMPATIBILITY_WRITE command part 2

Table 28. 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 16	see Section 9.3	4 bits

Table 29. 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 NTAG 213 TT, the following memory pages are valid Addr parameters to the COMPATIBILITY_WRITE command.

- page address 02h to 2Dh for NTAG 213 TT

Addressing a memory page beyond the limits above results in a NAK response from NTAG 213 TT.

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 NTAG 213 TT is in the ACTIVE state
  - writing to a page which address is equal or higher than AUTH0 results in a NAK response
- if NTAG 213 TT is in the AUTHENTICATED state
  - the COMPATIBILITY_WRITE command behaves the same as on a NTAG 213 TT without access protection

Writing to page 2Dh results in NAK if the TT_LOCK and/or TT_EN bits are set to 1.

NTAG 213 TT features tearing protected write operations to specific memory content. The following pages are protected against tearing events during a COMPATIBILITY_WRITE operation:

- page 02h containing static lock bits
- page 03h containing CC bits
- page 28h containing the additional dynamic lock bits for the NTAG 213 TT

10.6 READ_CNT

The READ_CNT command is used to read out the current value of the NFC one-way counter of the NTAG 213 TT. 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 16 and Table 30.

Table 31 shows the required timing.

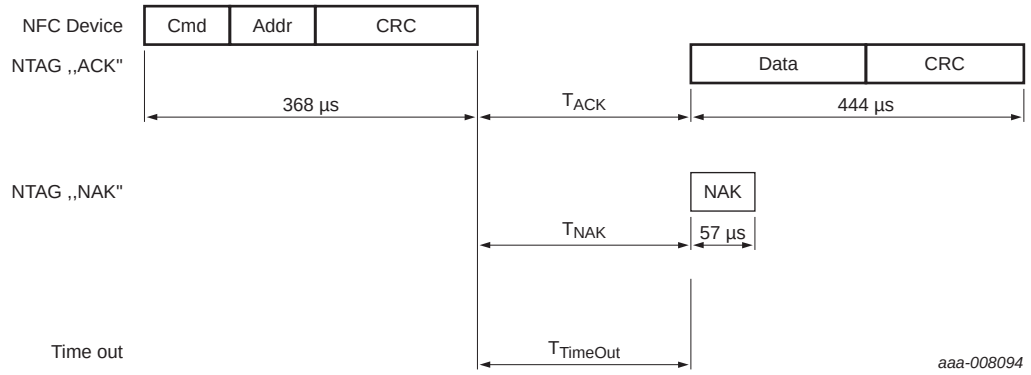


Fig 16. READ_CNT command

Table 30. 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 16	see Section 9.3	4 bits

Table 31. 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 NTAG 213 TT is in the ACTIVE state
  - Response to the READ_CNT command results in a NAK response
- if NTAG 213 TT 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 17 and Table 32.

Table 33 shows the required timing.

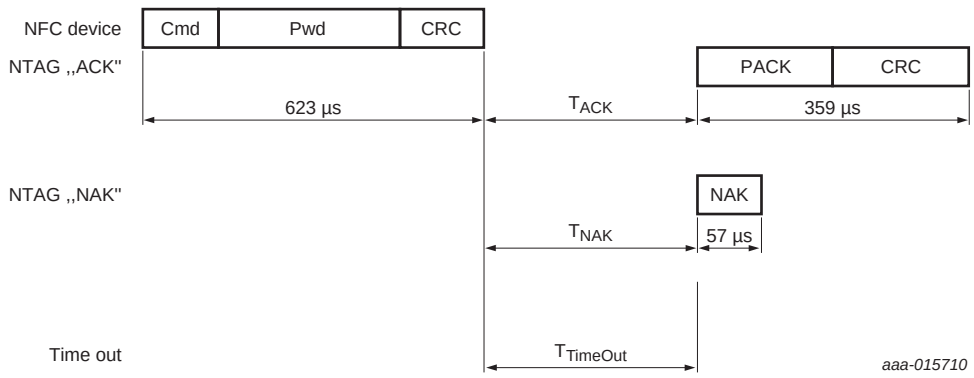


Fig 17. PWD_AUTH command

Table 32. 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 16	see Section 9.3	4 bits

Table 33. 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 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 the originality signature with the public key. The signature is programmed at chip production and cannot be changed afterwards. The command structure is shown in Figure 18 and Table 34.

Table 35 shows the required timing.

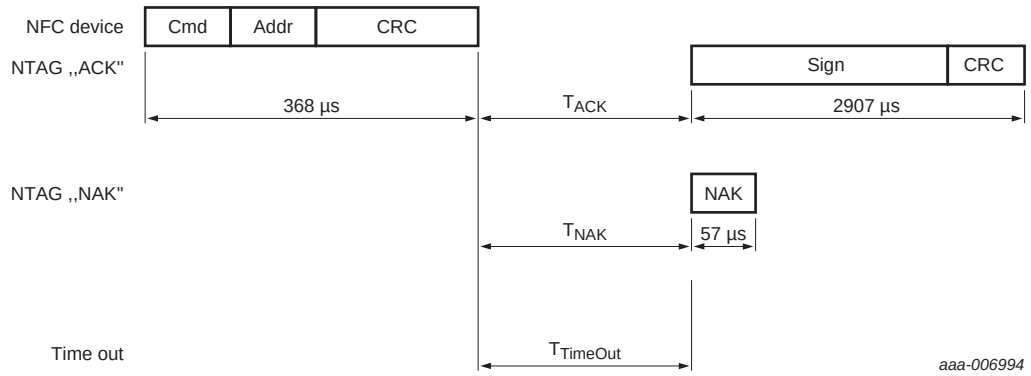


Fig 18. READ_SIG command

Table 34. 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 16	see Section 9.3	4 bits

Table 35. 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 that the signature value is provided in the following Application note (Ref. 5).

10.9 WRITE_SIG

The WRITE_SIG command allows the writing of a customized originality signature into the dedicated originality signature memory.

The WRITE_SIG command requires an originality signature block address, and writes 4 bytes of data into the addressed originality signature block. The WRITE_SIG command is shown in Figure 19 and Table 36.

Table 37 shows the required timing.

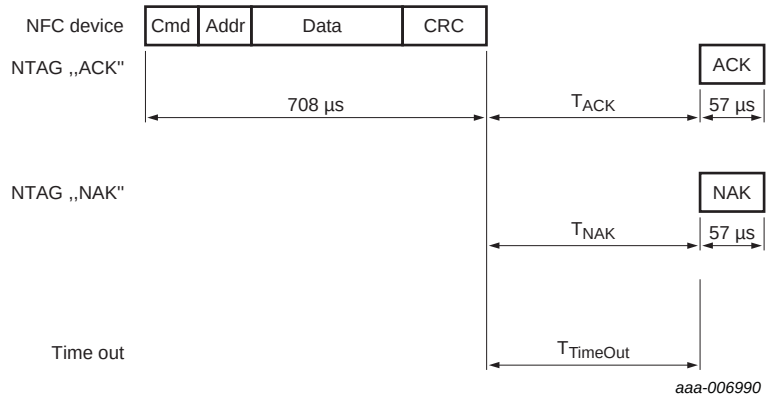


Fig 19. WRITE_SIG command

Table 36. WRITE_SIG command

Name	Code	Description	Length
Cmd	A9h	write one originality signature block	1 byte
Addr	-	block address	1 byte
CRC	-	CRC according to Ref. 1	2 bytes
Data	-	signature bytes to be written	4 bytes
NAK	see Table 16	see Section 9.3	4 bits

Table 37. WRITE_SIG timing

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

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

[1] Refer to Section 9.2 “Timings”.

In the initial state of NTAG 213 TT, the following originality signature blocks are valid Addr parameters to the WRITE_SIG command.

- originality signature block address 00h to 07h for NTAG 213 TT

Addressing a memory block beyond the limits above results in a NAK response from NTAG 213 TT.

Table 38. Blocks for the WRITE_SIG command

Originality signature block	byte 0	byte 1	byte 2	byte 3
00h				MSByte
01h				
...				
06h				
07h	LSByte			

10.10 LOCK_SIG

The LOCK_SIG command allows the user to unlock, lock or permanently lock the dedicated originality signature memory.

The originality signature memory can only be unlocked if the originality signature memory is not permanently locked.

Permanently locking of the originality signature with the LOCK-SIG command is irreversible and the originality signature memory can never be unlocked and reprogrammed again.

The LOCK_SIG command is shown in Figure 20 and Table 39.

Table 40 shows the required timing.

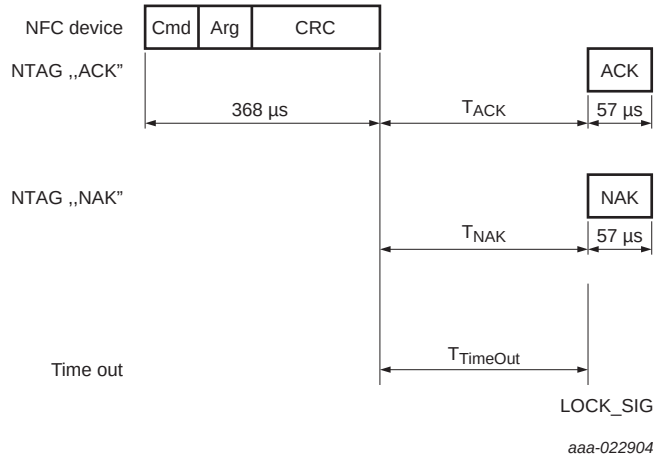


Fig 20. LOCK_SIG command

Table 39. LOCK_SIG command

Name	Code	Description	Length
Cmd	A9h	lock signature	1 byte
Arg	-	locking action	1 byte
		00h - unlock	1 byte
		01h - lock	1 byte
		02h - permanently lock	1 byte
CRC	-	CRC according to Ref. 1	2 bytes
NAK	see Table 16	see Section 9.3	4 bits

Table 40. LOCK_SIG timing

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

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

[1] Refer to Section 9.2 “Timings”.

10.11 READ_TT_STATUS

The READ_TT_Status command provides the information about the tag tamper status which is detected when the NTAG 213 TT is powered by an RF field. The response on The READ_TT_STATUS includes

- 4 byte Tag Tamper messages depend on the actual and previous tag tamper events and
- 1 byte about the actual status of the tag tamper wire during detected during startup

For details on those cases and the command structure, refer to Figure 21 and Table 41.

Table 42 shows the required timing.

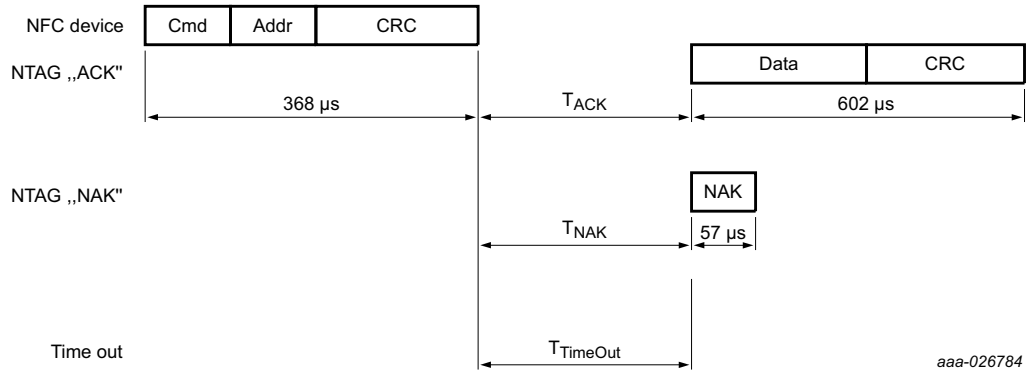


Fig 21. READ_TT_STATUS command

Table 41. READ_TT_STATUS command

Name	Code	Description	Length
Cmd	A4h	read Tag Tamper Status	1 byte
Addr	00h	RFU, is set to 00h	1 byte
CRC	-	CRC according to Ref. 1	2 bytes
Data	-	Tag Tamper Status	5 bytes
NAK	see Table 16	see Section 9.3	4 bits

Table 42. READ_TT_STATUS 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”.

Table 43. READ_TT_STAUS

Byte no.	Description	Value	Interpretation
0 - 3	TT_MESSAGE	30h	“0000” is returned, if the NTAG 213 TT has never detected the Tag Tamper as opened during the startup
		TT_MESSAGE	If the NTAG 213 TT has once detected the tag tamper wire as opened, it returns the data which have been programmed in page 2Dh (TT_MESSAGE)
4	Open/Close	43h	“C” if Tag Tamper was closed at current startup
		4Fh	“O” if Tag Tamper was open at current startup
		49h	“I” if Tag Tamper measurement was incorrect

Remark: The status of the tag tamper wire is only measured during the startup phase of the NTAG 213 TT.

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 44. 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_{ind}	maximum voltage on DP	-	0.5	V
T_{stg}	storage temperature	−55	125	°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 45. Characteristics

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
T_{amb}	ambient temperature		−25	-	70	°C
C_i	input capacitance		-	50.0	-	pF
f_i	input frequency		-	13.56	-	MHz
R_{on}	resistance tag taper closed	DP - GND	-	-	50	Ω
R_{off}	resistance tag tamper open	DP - GND	1 M	-	-	Ω
EEPROM characteristics						
t_{ret}	retention time	T_{amb} = 22 °C	10	-	-	year
$N_{endu(W)}$	write endurance	T_{amb} = 22 °C	100.000	-	-	cycle

13. Wafer specification

For more details on the wafer delivery forms see Ref. 6.

Table 46. Wafer specifications NTAG 213 TT

Wafer	
diameter	200 mm typical (8 inches)
maximum diameter after foil expansion	210 mm
thickness	
NT2L1x11G0DUD	120 μm ± 15 μm
NT2L1x11G0DUF	75 μm ± 10 μm
flatness	not applicable
Potential Good Dies per Wafer (PGDW)	79823
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 = 615 μm
	y = 625 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, DP = 60 μm × 60 μm
size variation	±5 μm
under bump metallization	sputtered TiW

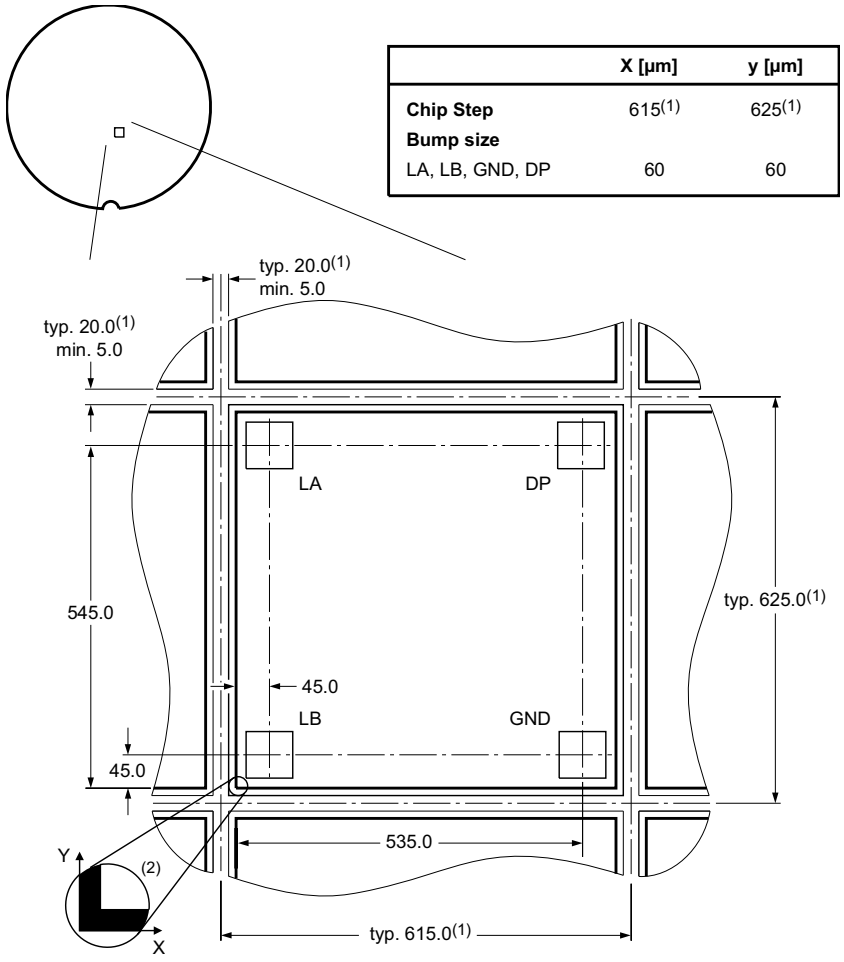
[1] The step size and the gap between chips may vary due to changing foil expansion

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.

14. Bare die outline

For more details on the wafer delivery forms, see Ref. 6.



(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-026783

Fig 22. Bare die outline NTAG 213 TT

15. Abbreviations

Table 47. 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

16. 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, Document number 2421**[1]

[5] **AN11350 NTAG21x Originality Signature Validation —** Application note, Document number 2604**[1]

[6] **General specification for 8" wafer on UV-tape; delivery types —** Delivery Type Description, Document number 1005**[1]

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

1. ** ... document version number

17. Revision history

Table 48. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
NT2H1311TT v.1.1	20170328	Objective data sheet	-	NTAG213 TT v.1.0
Modifications:	• Corrected minor version value in GET_VERSION command response (Table 21) • Added Section 13 “Wafer specification” • Editorial changing			
NTAG213_TT v.1.0	20150916	Objective data sheet	-	-
	• Initial version			

18. Legal information

18.1 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.

18.2 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.

18.3 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.

18.4 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. Purchase of NXP Semiconductors IC does not include a license to any NXP patent (or other IP right) covering combinations of those products with other products, whether hardware or software.

18.5 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.

NTAG — is a trademark of NXP B.V.

19. Contact information

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

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

20. Contents

1 General description 1
1.1 Contactless energy and data transfer 1
1.2 Simple deployment and user convenience 2
1.3 Security 2
1.4 NFC Forum Tag 2 Type compliance 2
1.5 Anticollision 2
2 Features and benefits 2
2.1 EEPROM 3
3 Applications 3
4 Quick reference data 4
5 Ordering information 4
6 Block diagram 4
7 Pinning information 5
7.1 Pinning 5
8 Functional description 6
8.1 Block description 6
8.2 RF interface 6
8.3 Data integrity 7
8.4 Communication principle 8
8.4.1 IDLE state 9
8.4.2 READY1 state 9
8.4.3 READY2 state 9
8.4.4 ACTIVE state 10
8.4.5 AUTHENTICATED state 10
8.4.6 HALT state 10
8.5 Memory organization 11
8.5.1 UID/serial number 11
8.5.2 Static lock bytes 12
8.5.3 Dynamic Lock Bytes 12
8.5.4 Capability Container (CC bytes) 14
8.5.5 Data pages 14
8.5.6 Memory content at delivery 15
8.5.7 Configuration pages 16
8.6 Tag Tamper feature 18
8.7 NFC counter function 19
8.8 ASCII mirror function 19
8.8.1 UID ASCII mirror function 20
8.8.2 NFC counter mirror function 21
8.8.3 Tag Tamper message mirror function 21
8.8.4 Example for UID, NFC counter and Tag Tamper message ASCII mirror 22
8.9 Password verification protection 26
8.9.1 Programming of PWD and PACK 26
8.9.2 Limiting negative verification attempts 27
8.9.3 Protection of special memory segments 27
8.10 Originality signature 27
8.10.1 Originality Signature at delivery 27
9 Command overview 29
9.1 NTAG 213 TT command overview 29
9.2 Timings 29
9.3 NTAG ACK and NAK 30
9.4 ATQA and SAK responses 30
10 NTAG commands 31
10.1 GET_VERSION 31
10.2 READ 33
10.3 FAST_READ 35
10.4 WRITE 37
10.5 COMPATIBILITY_WRITE 39
10.6 READ_CNT 41
10.7 PWD_AUTH 42
10.8 READ_SIG 43
10.9 WRITE_SIG 43
10.10 LOCK_SIG 45
10.11 READ_TT_STATUS 46
11 Limiting values 48
12 Characteristics 48
13 Wafer specification 49
13.1 Fail die identification 50
14 Bare die outline 51
15 Abbreviations 52
16 References 53
17 Revision history 54
18 Legal information 55
18.1 Data sheet status 55
18.2 Definitions 55
18.3 Disclaimers 55
18.4 Licenses 56
18.5 Trademarks 56
19 Contact information 56
20 Contents 57

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

Date of release: 28 March 2017
398311