NT2H2331G0

NTAG 223 DNA - NFC T2T compliant IC

Rev. 3.1 — 5 April 2023 | Product data sheet

1 General description

NTAG 223 DNA is an innovative security IC solution, compliant with NFC Forum Type 2 with 144 bytes of user memory. The technology uses advanced protection to support a broad range of NFC-based applications that can be trusted to protect products, services, and IoT-driven user experiences.

NTAG 223 DNA IC comes with a Secure Unique NFC (SUN) message authentication. The IC can automatically add its UID and incremental tap counter to the programmed NDEF (NFC Data Exchange Format) message through ASCII mirroring, and uses an AES-128 key to secure the message with a cryptographic message authentication code (CMAC). The SUN functionality supports advanced protection to verify a tag's authenticity and integrity, whilst also enabling secured unique user experiences served in real time. The IC uses AES-128 cryptography and is Common Criteria EAL3+ (AVA.VAN.2) targeted.

NTAG 223 DNA offers in addition an ECC-based originality signature to assure tag origin. The originality signature can be further customized and permanently locked during tag initialization.

The NTAG 223 DNA is compliant with NFC Forum Type 2 Tag ([1]) and ISO/IEC14443 Type A part 1 to 3 ([2]).

1.1 Contactless energy and data transfer

Communication to NTAG 223 DNA 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, general recommendations can be found in the NTAG antenna design guide (see [4]).

When NTAG 223 DNA 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.

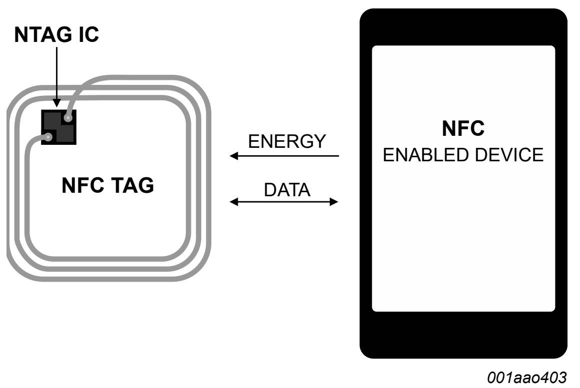


Figure 1. Contactless NTAG 223 DNA system

1.2 Simple deployment and better user experience

NTAG 223 DNA offers specific features designed to improve integration into physical objects and to enhance user experience:

- The fast read capability allows scanning the complete NDEF message with only one FAST_READ command, therefore reducing the overhead in high throughput production environments
- The RF performance allows for more flexibility in the choice of shape, dimension and material of form factors

1.3 Security

- EAL3+ AVA.VAN.2 Common Criteria certification
- Secure Unique NFC (SUN) message authentication for data authenticity and integrity protection
- Automatic NFC Tap Counter, which counts each tap
- NXP 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 with an option to customize and permanently lock
- 32-bit password protection to prevent unauthorized memory access

Note: NTAG 223 DNA comes with an external CC EAL3+ certification targeting basic attack potential (AVA_VAN.2). Hence, the contactless IC does not claim to be completely resistant. In case of broader protection is required, products with a higher security certification should be considered.

1.4 NFC Forum Tag 2 Type compliance

NTAG 223 DNA IC provides full compliance with the NFC Forum Tag 2 Type technical specification (see [2]) and enables NDEF data structure (see [3]).

1.5 Anti-collision

An anti-collision function allows operating more than one tag in the field simultaneously. The anti-collision 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)
- Automatic NFC counter triggered at the first read command after a reset
- Secure Unique NFC (SUN) message authentication feature implemented via ASCII mirroring of the UID, NFC counter and CMAC into the NDEF message in the user memory, which changes on every readout after a reset
- ECC-based originality signature, offering the option to customize and permanently lock the signature
- Fast read command
- True anti-collision
- 50 pF input capacitance

2.1 EEPROM

- 240 bytes organized in 60 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 memory access password protection with optional limit of unsuccessful attempts
- Anti-tearing support for capability container (CC), lock bits and NFC counter
- Pre-programmed ECC-based originality signature, offering the possibility for customizing and permanently locking the signature
- Setting for galvanic or capacitive tag tamper and sensing
- Data retention time of 10 years
- Write endurance 100.000 cycles

3 Applications

- **Advanced anti-counterfeiting protection**
  Reliably verify authenticity of physical goods, anytime, anywhere using an NFC enabled device. Also consider automated authentication of NFC tagged consumables and parts in embedded devices.
- **Improved supply chain visibility and control**
  Visibly help track products along the supply chain, and reduce grey market diversion and other fraud. Enable more transparent and secure supply chains.
- **Augmented user experiences**
  Use status awareness to prompt targeted messages, e.g. pre-/post-retail. Evolve the user experience by engaging with greater personalization, e.g. with tap-unique content and exclusive loyalty rewards.

4 Quick reference data

Table 1. Quick reference data

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
f_i	input frequency		-	13.56	-	MHz
C_i	input capacitance	T_{amb} = 22 °C, f_i = 13.56 MHz, 2.2 V RMS	-	50.0	-	pF
EEPROM characteristics						
t_{ret}	retention time	T_{amb} = 22 °C	10	-	-	year
$N_{endu(W)}$	write endurance	T_{amb} = 22 °C	100000	-	-	cycle

5 Ordering information

Table 2. Ordering information

Type number	Package		
	Name	Description	Version
NT2H2331G0DUD	FFC Bump	8 inch wafer, 120 μm thickness, on film frame carrier, electronic fail die marking according to SECS-II format, Au bumps, 144 bytes user memory, 50 pF input capacitance	-
NT2H2331G0DUF	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	-

6 Block diagram

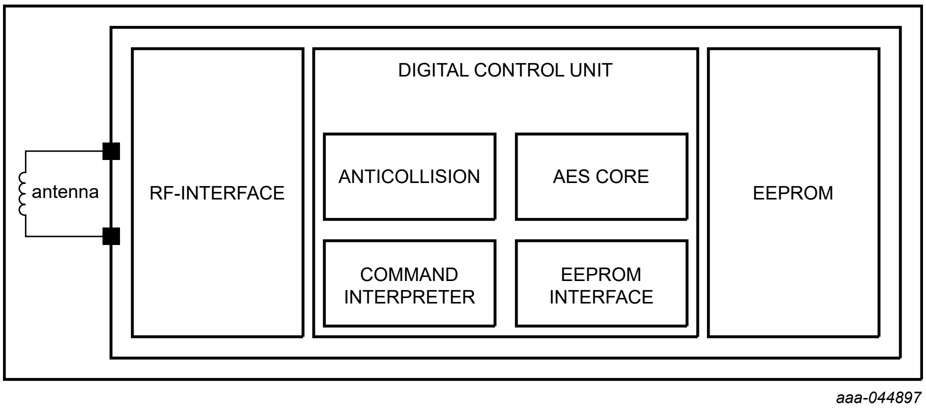


Figure 2. Block diagram of NTAG 223 DNA

7 Pinning information

7.1 Pinning

The pinning of the NTAG 223 DNA 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
TEST	TP	Test Pin
GND	GND	Ground Pin

8 Functional description

8.1 Block description

NTAG 223 DNA ICs consist of a 240 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 223 DNA.

No further external components are necessary. Refer to [4] for details on antenna design.

- RF interface:
  - modulator/demodulator
  - rectifier
  - clock regenerator
  - Power-On Reset (POR)
  - voltage regulator
- Anti-collision
- Command interpreter: processes memory access commands supported by the NTAG 223 DNA
- Crypto coprocessor: Advanced Encryption Standard (AES)
- EEPROM interface
- NTAG 223 DNA EEPROM : 240 bytes, organized in 60 pages of 4 bytes per page.
  - 10 bytes reserved for manufacturer data
  - 6 bytes used for the read-only locking mechanism and RFUI
  - 4 bytes available as capability container
  - 144 bytes user programmable read/write memory
  - 16 byte AES key
  - 60 bytes of configuration data and RFUI

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 except for REQA and WUPA commands. The LSB of the byte with the lowest address of the selected block is transmitted first.

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

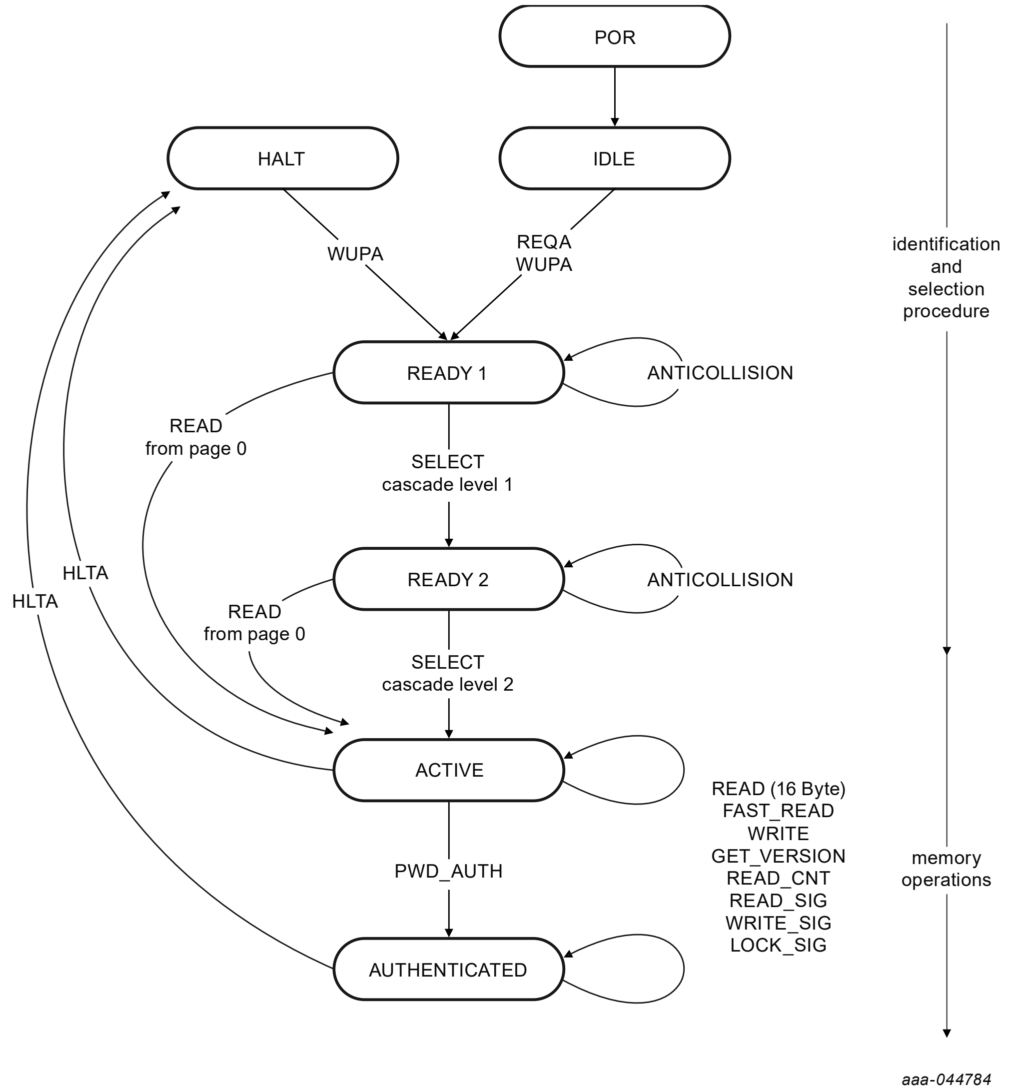
Following mechanisms are implemented in the contactless communication link between NFC device and NTAG to ensure very reliable data transmission:

- Bit count checking and bit coding to distinguish between "1", "0" and no information
- NAK1 response on user commands in case of parity or CRS error
- Parity bits for each byte

- 16-bit Cyclic Redundancy Check (CRC) according to ISO/IEC 14443-3, see [1], calculated over all preceding bytes in the same communication frame
- Channel monitoring (protocol sequence and bit stream analysis)
- Secure Unique NFC (SUN) CMAC mirror to protect the data integrity of the mirrored UID and NFC counter

8.4 Communication principle

The NFC device initiates the commands and the Digital Control Unit of the NTAG 223 DNA decodes 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.

Figure 3. State diagram

8.4.1 IDLE state

After a reset, NTAG 223 DNA 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 in this state is interpreted as an error and NTAG 223 DNA remains in the IDLE state.

After correctly executed HLTA command 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 or by a reset 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 223 DNA into READY2 state where the second part of the UID is resolved.
- READ command (from address 0): all anti-collision mechanisms are bypassed and the NTAG 223 DNA switches directly to the ACTIVE state.

Remark: The response of NTAG 223 DNA to the cascade level 1 SELECT command is a byte with b3 set to 1. In accordance with ISO/IEC 14443, this bit indicates that the anti-collision cascade procedure has not yet finished.

If more than one NTAG is in the NFC device field, a READ command from address 0 selects all NTAG 223 DNA 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 223 DNA returns to the IDLE or the HALT state.

8.4.3 READY2 state

In this state, NTAG 223 DNA 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 223 DNA to the cascade level 2 SELECT command is the Select Acknowledge (SAK) byte. In accordance with ISO/IEC 14443, this byte indicates if the anti-collision cascade procedure has finished. NTAG 223 DNA 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 223 DNA is in the NFC device field, a READ command from address 0 selects all NTAG 223 DNA devices. In this case, a collision occurs due to the different serial numbers.

Any other data received when the device is in state READY2 is interpreted as an error. Depending on its previous state, the NTAG 223 DNA returns to either the IDLE state or the HALT state.

8.4.4 ACTIVE state

Some memory operations and other functions like the originality signature read-out can be operated in the ACTIVE state.

The ACTIVE state is exited with the HLTA command. Upon reception of an HLTA command, the NTAG 223 DNA transits to the HALT state. An invalid command received when the device is in this state is interpreted as an error. Depending on its previous state, NTAG 223 DNA returns to either the IDLE state or the HALT state.

NTAG 223 DNA transits to the AUTHENTICATED state after successful password verification using the PWD_AUTH command.

8.4.5 AUTHENTICATED state

In this state, also operations on memory pages, which are configured as password protected, can be accessed on top of the operation that is allowed in ACTIVE state on pages that are not access protected.

The AUTHENTICATED state is exited with the HLTA command and upon reception NTAG 223 DNA transits to the HALT state. An invalid command received when the device is in this state is interpreted as an error. Depending on its previous state, NTAG 223 DNA returns to either the IDLE state or the HALT state.

8.4.6 HALT state

HALT and IDLE states constitute the two wait states implemented in NTAG 223 DNA. An already processed NTAG 223 DNA can be set into the HALT state using the HLTA command. In the anti-collision phase, this state helps the NFC device to distinguish between processed tags and tags yet to be selected. NTAG 223 DNA can only exit this state on execution of the WUPA command or reset. Any other data received when the device is in this state is interpreted as an error and NTAG 223 DNA TT state remains unchanged.

8.5 Memory organization

The EEPROM memory is organized in pages with 4 bytes per page. NTAG 223 DNA has 60 pages in total. The memory organization can be seen in Table 4, and the functionality of the different memory sections is described in the following sections.

Table 4. Memory organization NTAG 223 DNA

Page Addr		Byte number within a page				Description
Dec	Hex	0	1	2	3	
0	0h	serial number				Manufacturer data and static lock bits
1	1h	serial number				
2	2h	serial number	internal	lock bits	lock bits	
3	3h	Capability Container CC				Capability Container
4	4h	user memory				user memory
5	5h					
...						
38	26h					
39	27h					
40	28h	dynamic lock bits			RFUI	Dynamic lock bits
41	29h	CFG_0				Configuration pages
42	2Ah	CFG_1				
43	2Bh	PWD				
44	2Ch	PACK		RFUI		
45	2Dh	SUNCMAC_CFG	RFUI			

Table 4. Memory organization NTAG 223 DNA...*continued*

Page Addr		Byte number within a page				Description
Dec	Hex	0	1	2	3	
46	2Eh	RFUI				
47	2Fh	NFC_CNT_LIM			RFUI	
48	30h	RFUI				
...	...					
51	33h					
52	34h	SUNCMAC_KEY				
52	35h					
54	36h					
55	37h					
56	38h	RFUI				
57	39h	RFUI				
58	3Ah	RFUI				
59	3Bh	RFUI				

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

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.

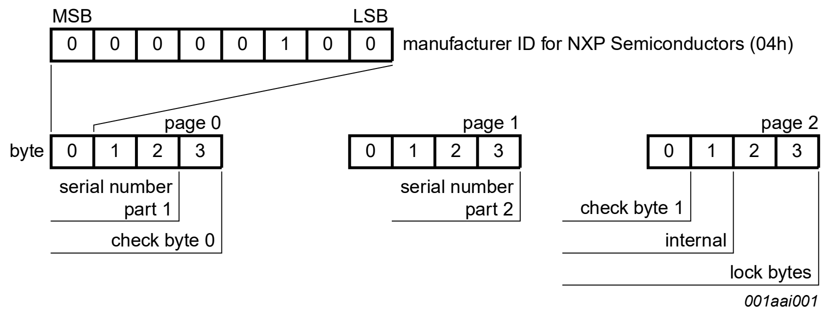


Figure 4. UID/serial number

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. The locked 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.

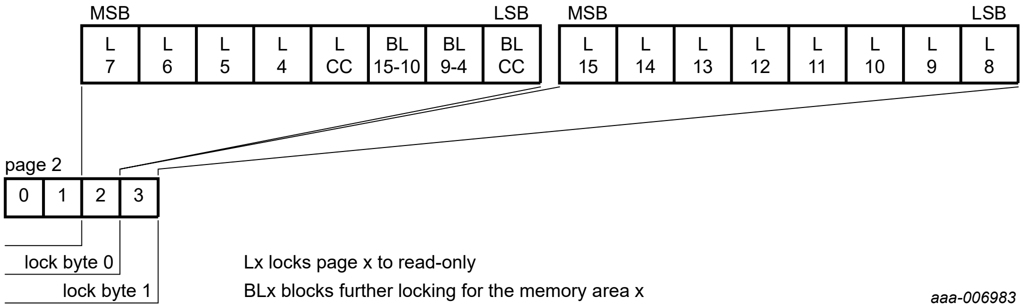


Figure 5. Static lock bytes 0 and 1 (page addresses are decimal)

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 command to block 02h, sets the static locking and block-locking bits. Data bytes 2 and 3 of the WRITE command, and the contents of the actual lock bytes stored in the memory, 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 content of bytes 0 and 1 of page 02h is unaffected by the corresponding data bytes of the 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 223 DNA starting at page address 10h until page 27h, so called dynamic lock bytes are used. Dynamic lock bytes are located at page 28h. Three lock bytes cover the memory area of 96 data bytes. The granularity of one lock bit is 2 pages for NTAG 223 DNA (Figure 6). The programming of dynamic lock bits is irreversible. If a bit is set to logic 1, it cannot be changed back to logic 0.

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

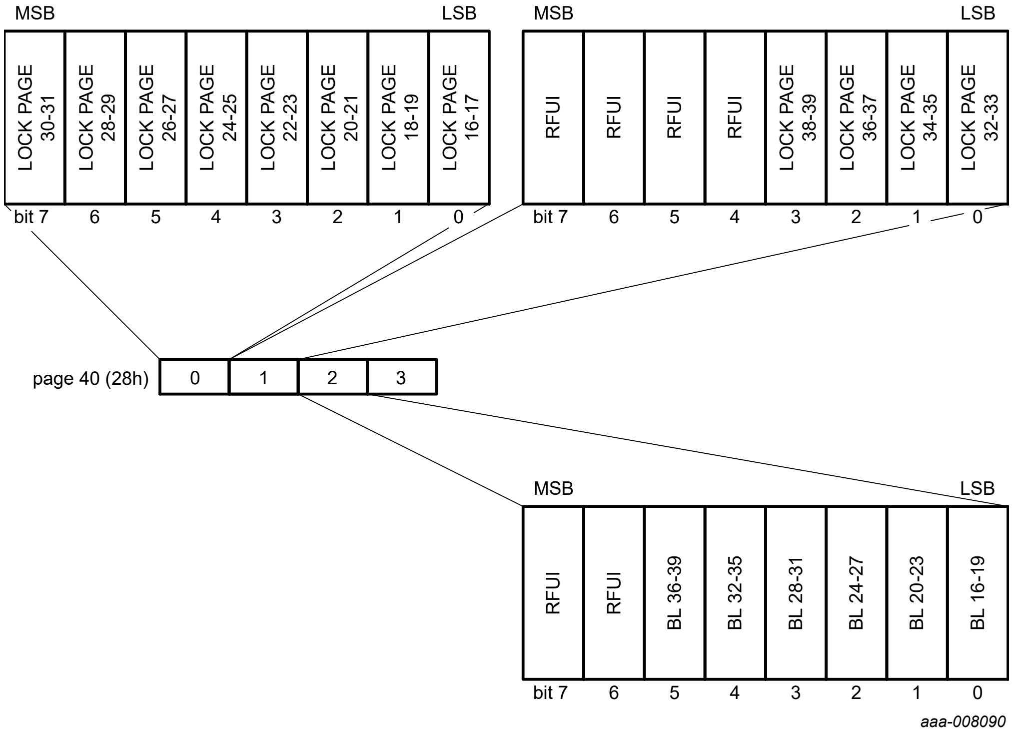


Figure 6. NTAG 223 DNA Dynamic lock bytes 0, 1 and 2 (page addresses are decimal)

The default value of the dynamic lock bytes is 00 00 00h. The value of byte 3 is always 00h 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 [2]). These bytes may be modified by a WRITE command.

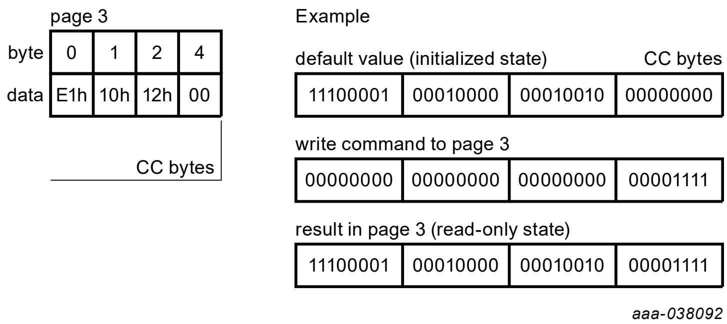


Figure 7. CC bytes example

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 bytes content. 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 5.

Table 5. NDEF memory size

IC	Value in byte 2	NDEF memory size
NTAG 223 DNA	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 223 DNA are the 144 byte 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 223 DNA are pre-programmed as defined in Table 6.

Table 6. Memory content at delivery NTAG 223 DNA

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 default content of the data pages from page 06h and onwards is not defined at delivery.

8.5.7 Configuration pages

Pages 29h to 3Bh for NTAG 223 DNA are used to configure the memory access restriction, to configure the ASCII mirror feature and tag tamper feature for galvanic or capacitive measurement. The location of the configuration elements is defined in Table 7.

Table 7. Configuration Pages

Byte number	Page Address		Byte number		
1	Dec	Hex	0	2	3
RFUI	41	29h	CFG_B0	MIRROR_PAGE	AUTH0
RFUI	42	2Ah	CFG_B1	AUTHLIM0	AUTHLIM1
PWD	43	2Bh	PWD		
PACK	44	2Ch	PACK	RFUI	RFUI
RFUI	45	2Dh	CMAC_CFG	RFUI	RFUI
RFUI	46	2Eh	RFUI	RFUI	RFUI
NFC_CNT_LIM	47	2Fh	NFC_CNT_LIM		RFUI
RFUI	48	30h	RFUI		

Table 7. Configuration Pages*...continued*

Byte number	Page Address		Byte number		
1	Dec	Hex	0	2	3
SUNCMAC_KEY	49	31h			
RFUI	50	32h			
RFUI	51	33h			
RFUI	52	34h	SUNCMAC_KEY		
RFUI	53	35h			
	54	36h			
	55	37h			
	56	38h	RFUI	RFUI	RFUI
	57	39h	RFUI	RFUI	RFUI
	58	3Ah	RFUI	RFUI	RFUI
	59	3Bh	RFUI	RFUI	RFUI

Table 8. CFG_B0 configuration byte

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

Table 9. User memory protection AUTH0 configuration byte

Bit number							
7	6	5	4	3	2	1	0
RFUI	AUTH0 [6:0]						

Table 10. CFG_B1 configuration byte

Bit number							
7	6	5	4	3	2	1	0
PROT	LOCK_ USR_CFG	RFUI	NFC_ CNT_EN	RFUI	RFUI	RFUI	RFUI

Table 11. AUTHLIM0 configuration byte

Bit number							
7	6	5	4	3	2	1	0
AUTH_LIM [7:0]							

Table 12. AUTHLIM1 configuration byte

Bit number							
7	6	5	4	3	2	1	0
RFUI						AUTH_ LIM [9]	AUTH_ LIM [8]

Table 13. CMAC_CFG configuration byte

Bit number							
7	6	5	4	3	2	1	0
LOCK_ SUNCMAC_ KEY	RFUI	BLOCK_ LOCK_KEY	RFUI				

Table 14. Configuration parameter descriptions

Field	Bit	Values at delivery	Description
MIRROR_EN	1	0b	Enables or disables the ASCII mirror functionality, if a valid MIRROR_PAGE address is set. This bit can be changed if LOCK_USR_CFG is not set. 0b ... ASCII mirror disabled 1b ... UID, NFC counter, TT and CMAC ASCII mirror enabled
MIRROR_BYTE	2	00b	2 bits define the byte position within the page defined by the MIRROR_PAGE address (beginning of mirror) where the ASCII mirror shall begin. These bits can be changed if LOCK_USR_CFG is not set.
MIRROR_PAGE	8	00h	MIRROR_PAGE address defines the page for the beginning of the mirroring. This byte can be changed if LOCK_USR_CFG is not set. A value >03h enables the ASCII mirror feature. The maximum valid value is 1Bh. If the ASCII mirror in given communication state is exceeding the accessible user memory, the ASCII mirror is disabled.
AUTH0	7	3Ch	AUTH0 defines the page address from which the password verification is required. Valid address range for byte AUTH0 is from 00h to 3Bh. If AUTH0 is set to a page address outside the valid address range, the AES authentication protection is effectively disabled, but still keeping password verification procedure working. This byte can be changed if LOCK_USR_CFG is not set.
PROT	1	1b	PROT bit is defining the type of protection of the password protected memory part assuming the AUTH0 byte value is within the range of 00h and 3Bh. This bit can be changed if LOCK_USR_CFG is not set. 0b ... write access only is protected by the password verification 1b ... read and write access is protected by the password verification
LOCK_USR_ CFG	1	0b	LOCK_USR_CFG permanently locks the configuration elements in blocks 29h, 2Ah, and 2Fh after subsequent reset. If the bit is set to 1b it cannot be set back to 0b. 0b ... configuration elements in blocks 29h, 2Ah, and 2Fh are not locked 1b ... configuration elements in blocks 29h, 2Ah, and 2Fh are permanently locked
NFC_CNT_EN	1	0b	NFC_CNT_EN enables or disables the incrementation of the NFC counter. This bit can be changed if LOCK_USR_CFG is not set.

Table 14. Configuration parameter descriptions*...continued*

Field	Bit	Values at delivery	Description
			0b ... NFC counter increment disabled 1b ... NFC counter increment enabled If the NFC counter increment is enabled, the NFC counter will be automatically increased by 1 at the first READ or FAST_READ command after a reset until the limiting value is reached (refer to Section 8.6)
AUTH_LIM	10	000h	Limitation of failed password verification attempts. Valid value range for byte AUTH_LIM is from 00h to 3FEh. AUTH_LIM can be changed if LOCK_USR_CFG is not set. 000h ... limiting of failed password verification disabled 001h - 3FEh ... maximum number of failed 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
LOCK_ SUNCMAC_KEY	1	0b	LOCK_SUNCMAC_KEY permanently locks the SUNCMAC_KEY in blocks 34h-37h. If the bit is set to 1b, it cannot be set back to 0b. 0b ... SUNCMAC_KEY in blocks 34h-37h is not locked 1b ... SUNCMAC_KEY in blocks 34h-37h is locked
BLOCK_LOCK_ KEY	1	0b	BLOCK_LOCK_KEY permanently locks the block 2Dh containing LOCK_ SUNCMAC_KEY. If the bit is set to 1b, it cannot be set back to 0b. 0b ... LOCK_SUNCMAC_KEY in block 2Dh is not locked 1b ... LOCK_SUNCMAC_KEY in block 2Dh is locked permanently
NFC_CNT_LIM	24	FFFFFFh	NFC_CNT_LIM defines the maximum value of the NFC counter (refer to Section 8.6). This bit can be changed if LOCK_USR_CFG is not set. 000000h … NFC counter limit is same as FFFFFFh 000001h - FFFFFFh … once the NFC counter has reached the NFC counter limit the counter will not be increased and will return with NAK on the first READ or FAST_READ command after a reset. After that the IC returns to the IDLE/HALT state.
SUNCMAC_KEY	128	All 0h	SUNCMAC_KEY refer to Section 8.8.
RFUI	-	not defined	Reserved for future use.

Remark: The LOCK_USR_CFG, LOCK_SUNCMAC_KEY, BLOCK_LOCK_KEY bits activate the permanent write protection of the corresponding configuration memory sections. If write protection is enabled, each write attempt to locked elements leads immediately to a NAK response.

8.6 NFC counter function

NTAG 223 DNA features an NFC counter function. This function enables NTAG 223 DNA to automatically increase the 24-bit counter value by 1, triggered by the first valid

- READ command or
- FAST-READ command

if the NFC counter value is smaller than FF FF FFh and the NFC_CNT_LIM (see Section 8.5.7) is disabled or higher than the NFC counter value after the NTAG 223 DNA tag is powered by an RF field.

Once the NFC counter has reached the maximum value of FF FF FFh hex or the NFC counter value is same or higher than the NFC_CNT_LIM value, the NFC counter does not increase anymore. On READ or FAST_READ after reset, the NAK answer is returned and NTAG 223 DNA becomes effectively unusable.

The NFC counter increment 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

8.7 ASCII mirror function

NTAG 223 DNA features an ASCII mirror function. This function enables NTAG 223 DNA to virtually mirror

- 7 byte UID (see Section 8.5.1)
- 3 byte NFC counter value (see Section 8.6)
- 8 byte SUNCMAC

into the physical memory of the IC in ASCII code. On the READ or FAST READ command to the involved user memory pages, NTAG 223 DNA 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 accessible user memory area, the data will not be mirrored.

Table 15. Required memory placeholder space for ASCII mirror

ASCII mirror and order	Required number of bytes in the physical memory
UID + NFC counter + TT message mirror + SUNCMAC	38 bytes (14 bytes for UID + 1 byte separation + 6 bytes NFC counter value + 1 byte separation + 16 byte SUNCMAC value)

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 MIRROR_EN set to 1b and MIRROR_PAGE value >03h.

The ASCII mirror elements are separated automatically with an "x" character (78h ASCII code).

Remark: Please note that the number of bytes (see Table 15) of the ASCII mirror shall not exceed the boundary of the user memory. Therefore it is required to use only valid values for MIRROR_BYTE and MIRROR_PAGE to ensure a proper functionality. If the ASCII mirror exceeds the user memory area, the ASCII mirrors shall be disabled.

8.7.1 UID ASCII mirror function

This function enables NTAG 223 DNA 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 223 DNA responds with the virtual memory content of the UID in ASCII code.

For an example see Table 16.

8.7.2 NFC counter mirror function

This function enables NTAG 223 DNA 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 223 DNA responds with the virtual memory content of the NFC counter in ASCII code.

For an example see Table 17.

Remark: To enable the NFC counter increment itself (see Section 8.7), the NFC_CNT_EN bit shall be set to 1b.

8.7.3 SUNCMAC mirror function

The SUNCMAC is calculated over the UID, NFC counter and Tag Tamper information. This function enables NTAG 223 DNA to virtually mirror the 8 byte SUNCMAC in ASCII code into the physical memory of the IC. The length of the SUNCMAC ASCII mirror requires 16 bytes to mirror the SUNCMAC in ASCII code.

To validate the mirrored data of UID, NFC counter and Tag Tamper information see Section 8.8

8.8 SUNCMAC

8.8.1 SUNCMAC calculation

The 8-byte SUNCMAC is calculated using AES according to the CMAC standard described in NIST Special Publication 800-38B (refer to [8]). Padding is applied according to this standard.

The MAC used in NTAG 223 DNA is truncated by using only the 8 even-numbered bytes out of the 16 bytes output as described NIST Special Publication 800-38B (refer to [8]) when represented in most-to-least-significant order.

The initialization vector used for the SUNCMAC computation is the zero byte IV as prescribed in NIST Special Publication 800-38B (refer to [8]).

The SUNCMAC is defined as follows:

SUNCMAC = MACt (SUNCMAC_KEY; DynamicSUNData)

with DynamicSUNData being the data in hex values (not mirrored ASCII values) of the UID and NFC.

The data from the mirrored information for the SUNCMAC calculation needs to be transferred as shown below.

14 Byte UID need to be transferred from ASCII to Hex value as shown in Table 16.

Table 16. UID mirrored data example

UID mirror data	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Byte 9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14
Mirrored data in hex	30	34	45	31	34	31	31	32	34	43	32	38	38	30
Mirrored ASCII character	0	4	E	1	4	1	1	2	4	C	2	8	8	0

For this example, the data of the UID for the SUNCMAC calculation are 04E141124C2880h.

6 Byte NFC counter mirror needs to be transferred from ASCII to Hex value as shown in Table 17.

Table 17. NFC counter mirrored data example

NFC counter mirror data	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6
Mirrored data in hex	30	30	30	34	41	46
Mirrored ASCII character	0	0	0	4	A	F

For this example, the data of the NFC Counter value for SUNCMAC calculation is 0004AFh.

For the example, the DynamicSUNData for the SUNCMAC calculation is 04E141124C28800004AFh.

8.8.2 Programming of the SUNCMAC key

The 16 bytes of the AES key are programmed to memory pages from 34h to 37h. The keys are stored in memory as shown in the table below. The key itself can be written during personalization or at any later stage using the WRITE command. For both commands, byte 0 is always sent first.

Table 18. SUNCMAC_KEY memory configuration

Page Address		Byte Number			
Dec	**Hex**	**0**	**1**	**2**	**3**
52	34h	K00	K01	K02	K03
53	35h	K04	K05	K06	K07
54	36h	K08	K09	K10	K11
55	37h	K12	K13	K14	K15

On example of SUNCMAC_KEY = 000102030405060708090A0B0C0D0E0Fh, the command sequence needed for key programming with WRITE command is:

- A2 34 0F 0E 0D 0C CRC
- A2 35 0B 0A 09 08 CRC
- A2 36 07 06 05 04 CRC
- A2 37 03 02 01 00 CRC

The memory content after those WRITE commands is shown in the table below:

Table 19. SUNCMAC_KEY memory configuration based on example configuration

Page Address		Byte Number			
Dec	**Hex**	**0**	**1**	**2**	**3**
52	34h	0F	0E	0D	0C
53	35h	0B	0A	09	08
54	36h	07	06	05	04
55	37h	03	02	01	00

The content of memory pages holding the SUNCMAC key can never be directly read neither by READ nor by FAST READ commands.

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

In the initial state of NTAG 223 DNA, password protection is disabled by an AUTH0 value of 3Ch. 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 NTAG223 DNA TT 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 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 LOCK_USR_CFG 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 223 DNA.

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 223 DNA.

8.9.2 Limiting failed authentication attempts

To reduce the risk on tag-only side channel attacks on AES key, the maximum allowed number of failed authentication attempts can be set using AUTH_LIM. This mechanism is disabled by setting AUTH_LIM to a value of 000h, which is also the initial state of NTAG 223 DNA.

If AUTH_LIM is not equal to 000h, each failed authentication attempt is internally counted and stored. The count operation features anti-tearing support. As soon as this internal counter reaches the number specified in AUTH_LIM, any further failed authentication attempt leads to a permanent locking of the protected part of the memory for the specified access rights. Specifically, each subsequent authentication fails independent if the authentication would be successful or not.

Any successful authentication, before reaching the limit of failed authentication attempts, decrements the internal counter by value 10h. In case the counter is at value of 10h or below the counter is reset.

8.9.3 Protection of configuration pages

The configuration pages can be protected by the 3-pass 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 before relevant configuration page address.

8.10 Originality signature

The NTAG 223 DNA offers a feature to verify the origin of a tag confidently, using the ECC-based originality signature stored in a hidden part of memory. The originality signature can be read with the READ_SIG command.

The purpose of the ECC originality check during (pre-)personalization is to protect customer investments by identifying mass penetration of non-NXP originated NTAG 223 DNA ICs into an infrastructure. As individual signatures can still be copied, it does not completely prevent hardware copy or emulation of individual NTAG 223 DNA ICs. As such, a valid signature is not a full guarantee. Therefore, this signature validation should be complemented with a check to detect if multiple ICs with the sameUID are being introduced in the system.

The NTAG 223 DNA provides the possibility to customize the originality signature to personalize the IC individually for specific application.

At delivery, the NTAG 223 DNA 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 afterward 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 223 DNA is programmed with an NXP digital signature based on standard Elliptic Curve Cryptography (curve name secp192r1), 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.

Each NTAG 223 DNA UID is signed with an NXP private key and the resulting 48-byte signature is stored in a hidden part of the NTAG 223 DNA 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 cryptolibrary OpenSSL, the tool domain parameters are set to secp192r1. It is defined within the standards for elliptic curve cryptography SEC ([7]).

Details on how to check that the NXP signature value is provided in following application note ([5]). It is foreseen to offer an online and offline way to verify originality of NTAG 223 DNA.

9 Command overview

NTAG 223 DNA activation follows part 2 and part 3 of ISO/IEC 14443 Type A. After NTAG 223 DNA has been selected, it can either be deactivated using the ISO/IEC 14443 HLTA command, or the NTAG 223 DNA commands (e.g. READ or WRITE) can be performed. For more details about the card activation, refer to [1]

9.1 NTAG 223 DNA command overview

All available commands for NTAG 223 DNA 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)
Anti-collision CL1	Anti-collision CL1	SDD_REQ CL1	93h 20h
Select CL1	Select CL1	SEL_REQ CL1	93h 70h
Anti-collision CL2	Anti-collision 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
READ_CNT	-	-	39h
PWD_AUTH	-	-	1Bh
READ_SIG	-	-	3Ch
WRITE_SIG	-	-	A9h
LOCK_SIG	-	-	ACh

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

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 [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 this 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 [1].

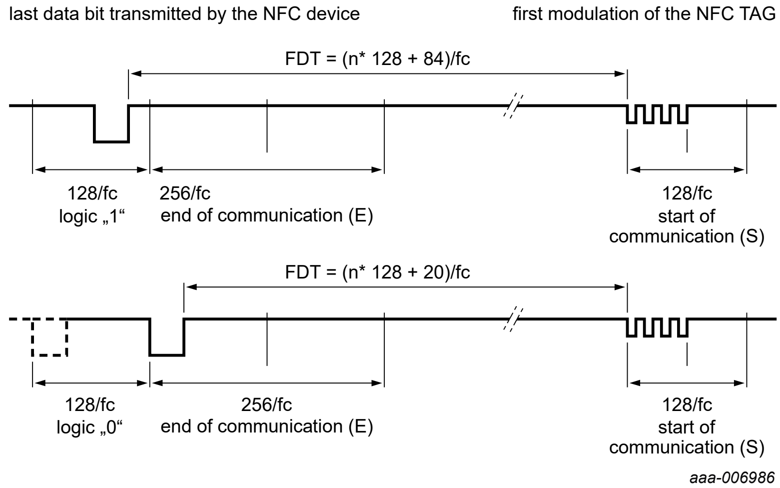


Figure 8. Frame Delay Time (from NFC device to NFC tag)

Remark: Due to the coding of commands, the measured command timings usually exclude (a part of) the end of communication. This factor shall be considered 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
4h	NAK for failed authentication counter overflow or NFC counter exceeding the limit
5h	NAK for EEPROM write error
6h	NAK if valid page indicators are corrupted for the given tearing protected pages. This can be due to memory content corruption caused by an attack.
7h	NAK for EEPROM write error

9.4 ATQA and SAK responses

NTAG 223 DNA 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 NTAG 223 DNA

		Bit number															
Sales type	Hex value	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
NT2H2331G0	00 44h	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0

Table 23. SAK response of the NTAG 223 DNA

		Bit number							
Sales type	**Hex value**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
NT2H2331G0	00h	0	0	0	0	0	0	0	0

Remark: The ATQA coding in bits 7 and 8 indicate the UID size according to Ref. 1 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 9 and Table 24.

Table 27 shows the required timing.

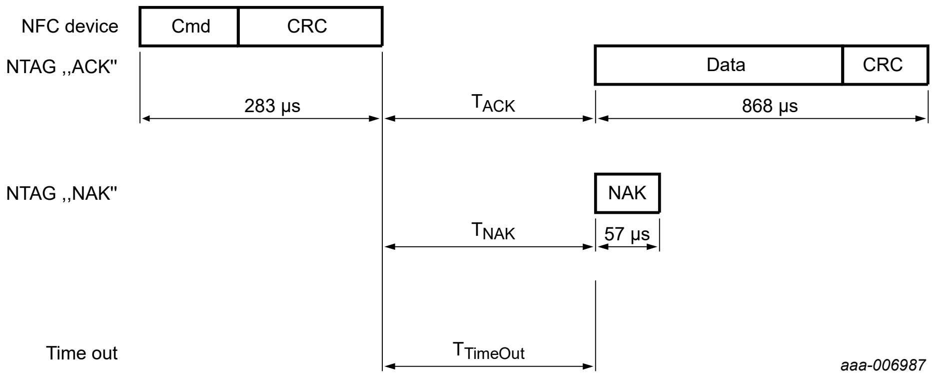


Figure 9. GET_VERSION command

Table 24. GET_VERSION command

Name	Code	Description	Length
Cmd	60h	Get product version	1 byte
CRC	-	CRC according to [1]	2 bytes

Table 25. GET_VERSION response

Name	Code	Description	Length
Data	-	Product version information (see Table 26)	8 bytes
CRC	-	CRC according to [1]	2 bytes
NAK	see Table 21	see Section 9.3	4 bits

Table 26. GET_VERSION data response for NTAG 223 DNA

Byte no.	Description	NTAG 223 DNA	Interpretation
0	fixed Header	00h	
1	vendor ID	04h	NXP Semiconductors
2	product type	04h	NTAG

Table 26. GET_VERSION data response for NTAG 223 DNA...*continued*

Byte no.	Description	NTAG 223 DNA	Interpretation
3	product subtype	02h	50 pF
4	major product version	04h	4
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 223 DNA 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.

Table 27. 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.

10.2 READ

The READ command requires a start page address, and returns 16 bytes of four NTAG 223 DNA pages. For example, if address (Addr) is 03h then the content pages 03h, 04h, 05h, 06h are returned. So call roll-over mechanism applies if the READ command address is near the end of the accessible memory area. The same mechanism also applies if at least part of the addressed pages is within a password protected area. For details on the command structure, refer to Figure 10 and Table 28.

Table 30 shows the required timing.

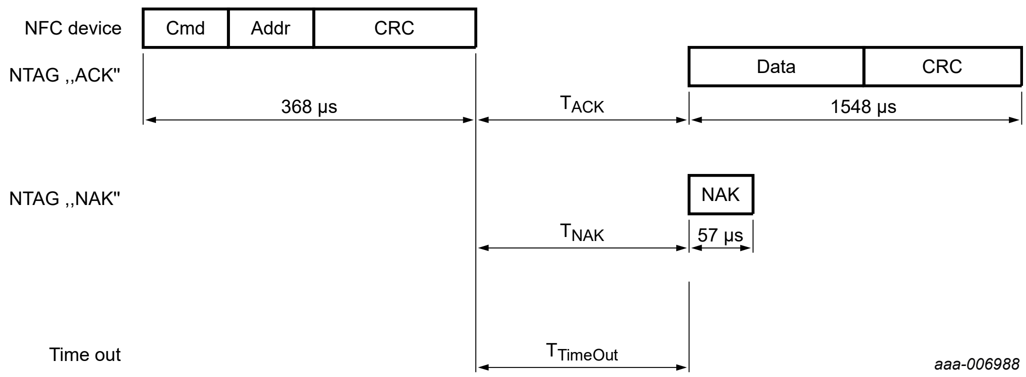


Figure 10. READ command

Table 28. READ command

Name	Code	Description	Length
Cmd	30h	read four pages	1 byte

Table 28. READ command...*continued*

Name	Code	Description	Length
Addr	-	start page address	1 byte
CRC	-	CRC according to [1]	2 bytes

Table 29. READ response

Name	Code	Description	Length
Data	-	Data content of the addressed pages	16 bytes
CRC	-	CRC according to [1]	2 bytes
NAK	see Table 21	see Section 9.3	4 bits

Table 30. 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.

In the initial state of NTAG 223 DNA, all memory pages in the range from 00h until 3Bh are allowed as Addr parameter to the READ command.

Addressing a memory page beyond address 3Bh results in a NAK response from NTAG 223 DNA.

A roll-over mechanism is implemented to continue reading from page 00h once the end of the accessible memory is reached. For example, reading from address 39h on an NTAG 223 DNA results in pages 39h, 3Ah, 3Bh and 00h being returned.

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

- if NTAG 223 DNA 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 one page before the AUTH0 defined page
- if NTAG 223 DNA is in the AUTHENTICATED state
  - the READ command behaves like on an NTAG 223 DNA without access protection

Remark: PWD and PACK values cannot 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 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 either start or end address is out of the accessible area, NTAG 223 DNA replies a NAK. For details on the command structure, refer to Figure 11 and Table 31.

Table 33 shows the required timing.

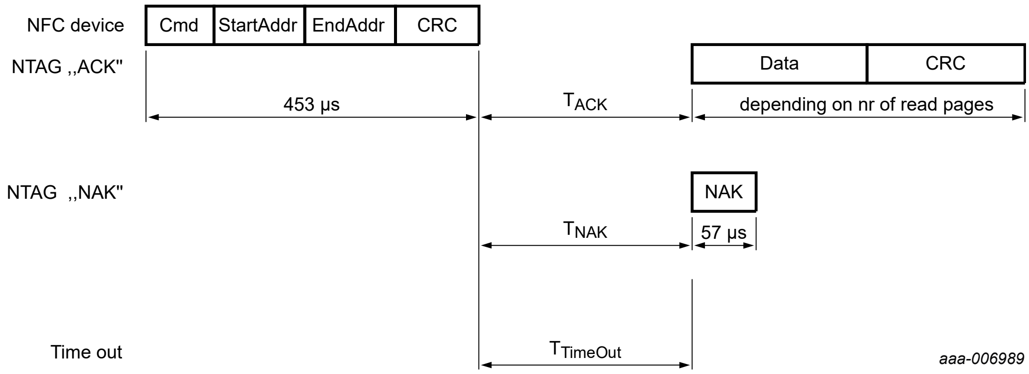


Figure 11. FAST_READ command

Table 31. 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 [1]	2 bytes

Table 32. FAST_READ response

Name	Code	Description	Length
Data	-	data content of the addressed pages	n*4 bytes
CRC	-	CRC according to [1]	2 bytes
NAK	see Table 21	see Section 9.3	4 bits

Table 33. 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.

In the initial state of NTAG 223 DNA, all memory pages in the range from 00h to 3Bh are allowed as StartAddr parameter to the FAST_READ command.

Addressing a memory page beyond address 3Bh results in a NAK response from NTAG 223 DNA.

The EndAddr parameter must be equal to or higher than the StartAddr otherwise NAK response is provided.

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

- if NTAG 223 DNA is in the ACTIVE state
  - if any requested page address is equal or higher than AUTH0 a NAK is replied
- if NTAG 223 DNA is in the AUTHENTICATED state
  - the FAST_READ command behaves like on an NTAG 223 DNA without access protection

Remark: PWD and PACK values cannot be read out of the memory. When reading from 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 accessible memory. 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 223 DNA page. The WRITE command is shown in Figure 12 and Table 34.

Table 36 shows the required timing.

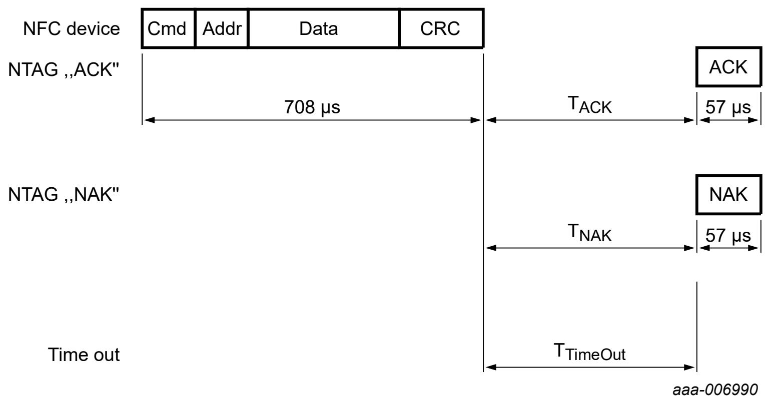


Figure 12. WRITE command

Table 34. WRITE command

Name	Code	Description	Length
Cmd	A2h	write one page	1 byte
Addr	-	page address	1 byte
Data	-	data	4 bytes
CRC	-	CRC according to [1]	2 bytes

Table 35. WRITE response

Name	Code	Description	Length
ACK/NAK	see Table 21	see Section 9.3	4 bits

Table 36. 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.

In the initial state of NTAG 223 DNA, page address 02h to 3Bh are valid Addr parameters to the WRITE command.

Addressing a memory page beyond address 3Bh results in a NAK response from NTAG 223 DNA.

Pages which are locked against writing cannot be reprogrammed using WRITE command. The locking mechanisms include static and dynamic lock bits as well as specific lock bits of different configuration elements.

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

- if NTAG 223 DNA is in the ACTIVE state
  - writing to a page which address is equal or higher than AUTH0 results in a NAK response
- if NTAG 223 DNA is in the AUTHENTICATED state
  - the WRITE command behaves like on an NTAG 223 DNA without access protection

NTAG 223 DNA 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 223 DNA

10.5 READ_CNT

The READ_CNT command is used to read out the current value of the NFC one-way counter of the NTAG 223 DNA. The command has a single argument specifying the counter number and returns the 24-bit counter value of the corresponding counter. The command structure is shown in Figure 13 and Table 37.

Table 39 shows the required timing.

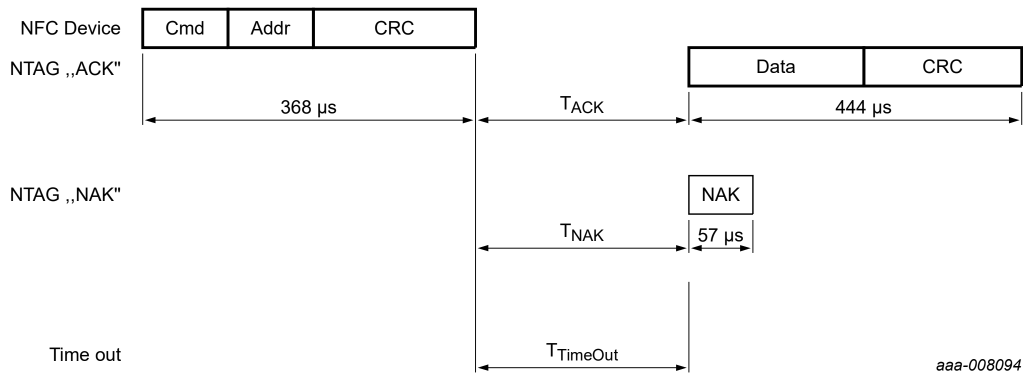


Figure 13. READ_CNT command

Table 37. READ_CNT command

Name	Code	Description	Length
Cmd	39h	read counter	1 byte
Addr	02h	NFC counter address	1 byte
CRC	-	CRC according to [1]	2 bytes

Table 38. READ_CNT response

Name	Code	Description	Length
Data	-	counter value	3 bytes
CRC	-	CRC according to [1]	2 bytes
NAK	see Table 21	see Section 9.3	4 bits

Table 39. 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.

10.6 PWD_AUTH

A protected memory area can be accessed only after a successful password verification using the PWD_AUTH command. The AUTH0 configuration byte defines the protected area. It specifies the first page that the password mechanism protects. The level of protection can be configured using the PROT bit either for write protection or read/write protection. The PWD_AUTH command takes the password as parameter and, if successful, returns the password authentication acknowledge, PACK. By setting the AUTH_LIM 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 14 and Table 40.

Table 42 shows the required timing.

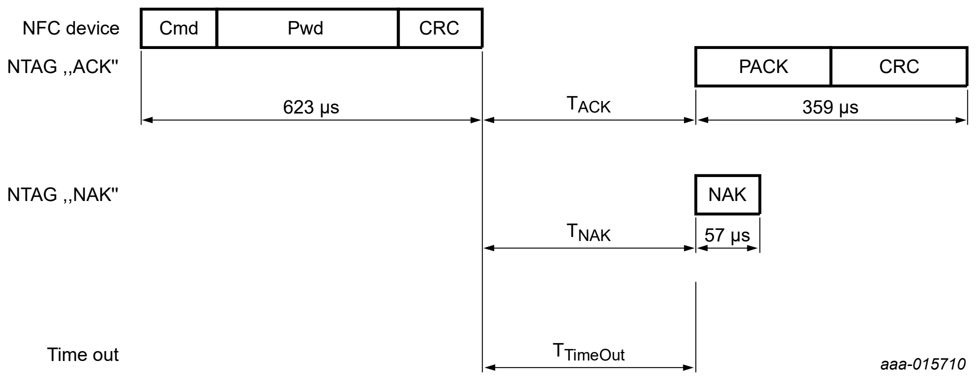


Figure 14. PWD_AUTH command

Table 40. PWD_AUTH command

Name	Code	Description	Length
Cmd	1Bh	password authentication	1 byte
Pwd	-	password	4 bytes
CRC	-	CRC according to [1]	2 bytes

Table 41. PWD_AUTH response

Name	Code	Description	Length
PACK	-	password authentication acknowledge	2 bytes
CRC	-	CRC according to [1]	2 bytes
NAK	see Table 21	see Section 9.3	4 bits

Table 42. 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.

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

10.7 READ_SIG

The READ_SIG command returns an IC-specific, 48 byte ECC signature, to verify the originality signature with the public key. The signature is pre-programmed at chip production and can be changed (see Section 10.8) if the originality signature has been unlocked with the LOCK_SIG command (see Section 10.9). The command structure is shown in Figure 15 and Table 43.

Table 45 shows the required timing.

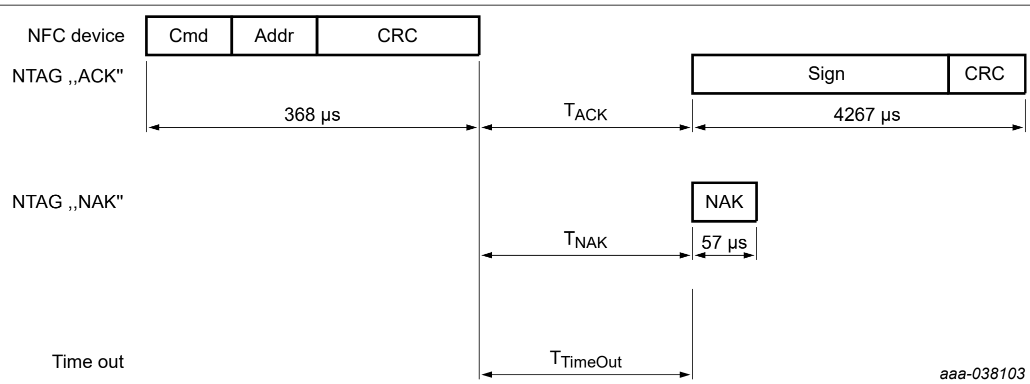


Figure 15. READ_SIG command

Table 43. 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 [1]	2 bytes

Table 44. READ_SIG response

Name	Code	Description	Length
Signature	-	ECC signature	48 bytes
CRC	-	CRC according to [1]	2 bytes
NAK	see Table 21	see Section 9.3	4 bits

Table 45. 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.

Details on how to check that the signature value is provided in the following Application note ([5]).

10.8 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 (see Table 49), and writes 4 bytes of data into the addressed originality signature block. The WRITE_SIG command is shown in Figure 16 and Table 46.

Table 48 shows the required timing.

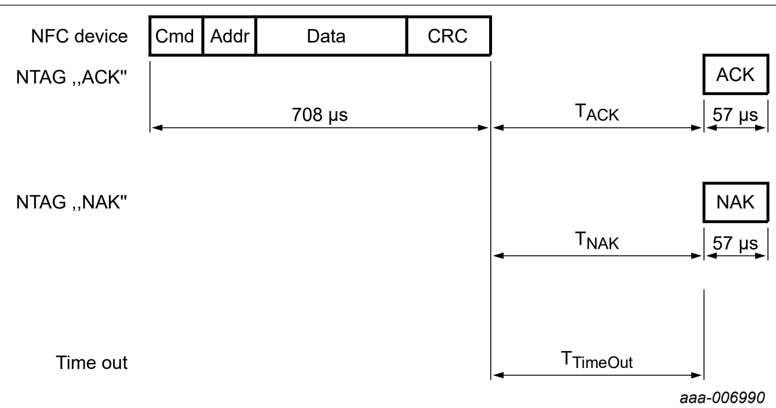


Figure 16. WRITE_SIG command

Table 46. WRITE_SIG command

Name	Code	Description	Length
Cmd	A9h	write one originality signature block	1 byte
Addr	-	block address	1 byte
Data	-	signature bytes to be written	4 bytes
CRC	-	CRC according to [1]	2 bytes

Table 47. WRITE_SIG response

Name	Code	Description	Length
ACK/NAK	see Table 21	see Section 9.3	4 bits

Table 48. 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.

In the initial state of NTAG 223 DNA, the originality signature block address 00h to 0Bh are valid Addr parameters to the WRITE_SIG command.

Addressing a memory block beyond address 0Bh results in a NAK response from NTAG 223 DNA.

Table 49. Blocks for the WRITE_SIG command

Originality signature block	byte 0	byte 1	byte 2	byte 3
00h	LSByte			
01h				
...				
0Ah				
0Bh				MSByte

10.9 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 17 and Table 50.

Table 52 shows the required timing.

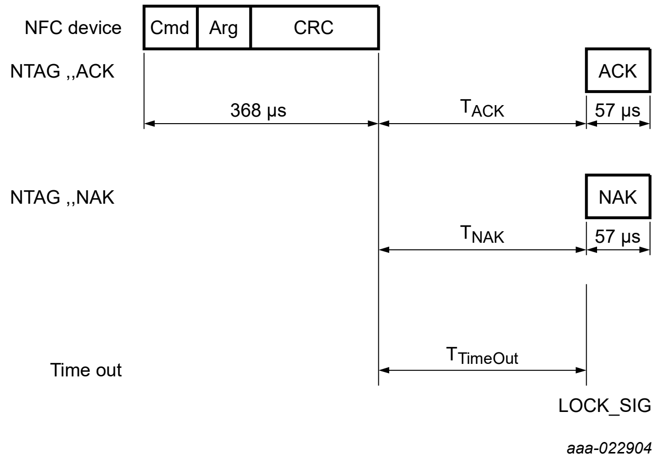


Figure 17. LOCK_SIG command

Table 50. LOCK_SIG command

Name	Code	Description	Length
Cmd	ACh	lock signature	1 byte
Arg	-	locking action	1 byte
		00h - unlock	
		01h - lock	
		02h - permanently lock	
CRC	-	CRC according to [1]	2 bytes

Table 51. LOCK_SIG response

Name	Code	Description	Length
ACK/NAK	see Table 21	see Section 9.3	4 bits

Table 52. 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.

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 53. Limiting values

In accordance with the Absolute Maximum Rating System (IEC 60134).

Symbol	Parameter		Min	Max	Unit
$P_{d,max}$	maximum power dissipation		-	120	mW
$I_{LA-LB,max}$	maximum input current		-	40	mA
T_{stg}	storage temperature		-55	125	°C
T_{amb}	ambient temperature		-25	+70	°C
V_{ESD}	electrostatic discharge voltage on LA/LB, DP/GND	[1]	-	2	kV

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

CAUTION

This device has limited built-in ElectroStatic Discharge (ESD) protection. The leads should be shorted together or the device placed in conductive foam during storage or handling to prevent electrostatic damage to the gates.

12 Characteristics

Table 54. Electrical Characteristics

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
f_i	input frequency		-	13.56	-	MHz
C_i	input capacitance[1]	T_{amb} = 25 °C	-	50.0	-	pF
EEPROM characteristics						
t_{ret}	retention time	T_{amb} = 22 °C	10	-	-	year
$N_{endu(W)}$	write endurance	T_{amb} = 22 °C	100.000	-	-	cycle

[1] f_i = 13.56 MHz; 2.2 V RMS

13 Wafer specification

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

Table 55. Wafer specifications NTAG 223 DNA

Wafer	
diameter	200 mm typical (8 inches)
maximum diameter after foil expansion	210 mm
thickness NT2H2331G0DUD NT2H2331G0DUF	 120 µm ± 15 µm 75 µm ± 10 µm
flatness	not applicable
Potential Good Dies per Wafer (PGDW)	42521
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 = 832 µm
	y = 832 µm
gap between chips[1]	typical = 20 µm
	minimum = 5 µm
Passivation	
type	sandwich structure
material	PSG / nitride
thickness	500 nm / 600 nm
Au bump (substrate connected to VSS)	
material	> 99.9 % pure Au
hardness	35 to 80 HV 0.005
shear strength	> 70 MPa
height	18 µm
height uniformity	within a die = ±2 µm
	within a wafer = ±3 µm
	wafer to wafer = ±4 µm
flatness	minimum = ±1.5 µm
size	LA, LB, GND, TP = 80 µm × 80 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 Delivery

The customer purchasing a product of the NTAG 223 DNA family has to make sure that they receive the evaluated version. This section describes the measures that are needed to ensure delivery of the evaluated version.

The evaluated version of the NTAG 223 DNA can be ordered from NXP by referencing the respective commercial type name as listed in Section 5.

NXP offers two ways of delivery of the product:

1. The customer collects the product themselves at the NXP site.
2. The product is sent by NXP to the customer and protected by special measures.

These methods are described in Section 14.2 and Section 14.3 respectively.

14.1 Delivery as a wafer

When the product is delivered as wafer, there reside functional and non-functional ICs on the wafer. The non-functional ICs cannot be used but have to be handled securely, too. These ICs must be destroyed to such an extent that no analysis or misuse is possible after destruction. The non-functional ICs (scrap) shall be handled secure until the destruction.

Information about non-functional items is accessible via the eMAP-Portal (http://wmt.nxp.com). The Access sheet with the Login data is enclosed with the delivery to allow the download of the electronic wafer map file. In this case, the information about non-functional ICs is stored in a so-called wafer map file. The electronic wafer map file covers the electrical test results and additionally the results of mechanical/visual inspection.

14.2 Delivery Method One: The customer collects the product themselves

The customer fetches the product from the following location:

NXP Semiconductors (Thailand)

303 Chaengwattana Rd.Laksi

Bangkok

10210 Thailand

This method guarantees that the customer gets authentic products.

14.3 Delivery Method Two: The Product is sent by NXP and protected by special measures

To guarantee that the product is not manipulated during the delivery, NXP has defined three security measures:

1. The product is delivered in parcels sealed with special tapes. The customer can examine these tapes in order to make sure that they have not been manipulated.
2. The customer shall identify the product as described in Section 10.1.
3. The customer should check the originality by verification of the Originality Signature Section 8.10.1.

These measures shall be applied to ensure that a genuine chip is in use. The product is delivered directly to the customer or via the Global Distribution Center:

NXP Semiconductors Netherlands B.V.

(Global Distribution Centre)

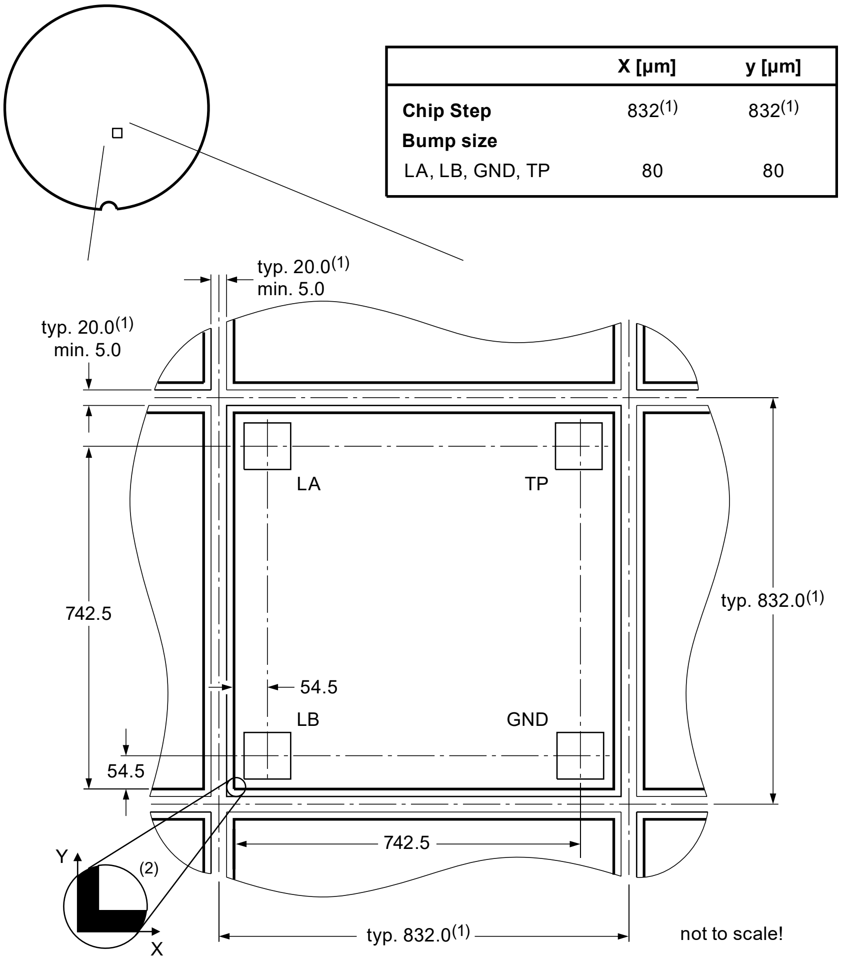
c/o CEVA Logistics (Malaysia) Sdn Bhd

Lot 9A Jalan Tiang U8/92, Bukit Jelutong Industrial Park, 40150 Shah Alam, Selangor Darul Ehsan, MALAYSIA

15 Bare die outline

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

	X [µm]	y [µm]
Chip Step	832(1)	832(1)
Bump size		
LA, LB, GND, TP	80	80



(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-050978

Figure 18. Bare die outline NTAG 223 DNA

16 Abbreviations

Table 56. 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
MSB	Most 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

17 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 NTAG 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

[8] **NIST Special Publication 800-38B** - National Institute of Standards and Technology (NIST). Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. https://csrc.nist.gov/publications/detail/sp/800-38b/final

1 ** ... document version number

18 Revision history

Table 57. Revision history

Document ID	Release date	Data sheet status	Supersedes
NT2H2331G0 v.3.1	20230405	Product data sheet	NT2H2331G0 v.3.0
Modifications:	• Bump size changed from 60 µm to 80 µm in Section 13 and Figure 18		
NT2H2331G0 v.3.0	20220218	Product data sheet	NT2H2331G0 v.2.0
Modifications:	• Data sheet status changed to "Product data sheet", security status changed to "Company public"		
NT2H2331G0 v.2.0	20220205	Preliminary data sheet	NT2H2331G0 v.1.1
Modifications:	• Editorial changes		
NT2H2331G0 v.1.1	20211220	Objective data sheet	NT2H2331G0 v.1.0
Modifications:	• Updated section "General description" (see Section 1) • Updated section "Applications" (see Section 3) • PGDW updated in section "Wafer specification" (see Table 55)		
NT2H2331G0 v.1.0	20211125	Objective data sheet	NT2H2331G0 v.0.6
Modifications:	• General update		
NT2H2331G0 v.0.6	20201028	Objective data sheet	
Modifications:	• First draft		

19 Legal information

19.1 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.

19.2 Definitions

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

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.

19.3 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.

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.

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.

Suitability for use in 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.

NXP B.V. - NXP B.V. is not an operating company and it does not distribute or sell products.

19.4 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.

19.5 Trademarks

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

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

NTAG — is a trademark of NXP B.V.

Tables

Tab. 1. Quick reference data 6
Tab. 2. Ordering information 7
Tab. 3. Pin allocation table 9
Tab. 4. Memory organization NTAG 223 DNA 13
Tab. 5. NDEF memory size 17
Tab. 6. Memory content at delivery NTAG 223 DNA 17
Tab. 7. Configuration Pages 17
Tab. 8. CFG_B0 configuration byte 18
Tab. 9. User memory protection AUTH0 configuration byte 18
Tab. 10. CFG_B1 configuration byte 18
Tab. 11. AUTHLIM0 configuration byte 18
Tab. 12. AUTHLIM1 configuration byte 19
Tab. 13. CMAC_CFG configuration byte 19
Tab. 14. Configuration parameter descriptions 19
Tab. 15. Required memory placeholder space for ASCII mirror 21
Tab. 16. UID mirrored data example 22
Tab. 17. NFC counter mirrored data example 22
Tab. 18. SUNCMAC_KEY memory configuration 23
Tab. 19. SUNCMAC_KEY memory configuration based on example configuration 23
Tab. 20. Command overview 26
Tab. 21. ACK and NAK values 27
Tab. 22. ATQA response of the NTAG 223 DNA 27
Tab. 23. SAK response of the NTAG 223 DNA 28
Tab. 24. GET_VERSION command 29
Tab. 25. GET_VERSION response 29
Tab. 26. GET_VERSION data response for NTAG 223 DNA 29
Tab. 27. GET_VERSION timing 30
Tab. 28. READ command 30
Tab. 29. READ response 31
Tab. 30. READ timing 31
Tab. 31. FAST_READ command 32
Tab. 32. FAST_READ response 32
Tab. 33. FAST_READ timing 32
Tab. 34. WRITE command 33
Tab. 35. WRITE response 33
Tab. 36. WRITE timing 34
Tab. 37. READ_CNT command 35
Tab. 38. READ_CNT response 35
Tab. 39. READ_CNT timing 35
Tab. 40. PWD_AUTH command 36
Tab. 41. PWD_AUTH response 36
Tab. 42. PWD_AUTH timing 36
Tab. 43. READ_SIG command 37
Tab. 44. READ_SIG response 37
Tab. 45. READ_SIG timing 37
Tab. 46. WRITE_SIG command 38
Tab. 47. WRITE_SIG response 38
Tab. 48. WRITE_SIG timing 38
Tab. 49. Blocks for the WRITE_SIG command 38
Tab. 50. LOCK_SIG command 39
Tab. 51. LOCK_SIG response 39
Tab. 52. LOCK_SIG timing 39
Tab. 53. Limiting values 40
Tab. 54. Electrical Characteristics 41
Tab. 55. Wafer specifications NTAG 223 DNA 42
Tab. 56. Abbreviations and symbols 47
Tab. 57. Revision history 49

Figures

Fig. 1. Contactless NTAG 223 DNA system 1
Fig. 2. Block diagram of NTAG 223 DNA 8
Fig. 3. State diagram 11
Fig. 4. UID/serial number 14
Fig. 5. Static lock bytes 0 and 1 (page addresses are decimal) 15
Fig. 6. NTAG 223 DNA Dynamic lock bytes 0, 1 and 2 (page addresses are decimal) 16
Fig. 7. CC bytes example 16
Fig. 8. Frame Delay Time (from NFC device to NFC tag) 27
Fig. 9. GET_VERSION command 29
Fig. 10. READ command 30
Fig. 11. FAST_READ command 32
Fig. 12. WRITE command 33
Fig. 13. READ_CNT command 34
Fig. 14. PWD_AUTH command 35
Fig. 15. READ_SIG command 36
Fig. 16. WRITE_SIG command 37
Fig. 17. LOCK_SIG command 39
Fig. 18. Bare die outline NTAG 223 DNA 46

Contents

1	**General description**	**1**
1.1	Contactless energy and data transfer	1
1.2	Simple deployment and better user experience	2
1.3	Security	3
1.4	NFC Forum Tag 2 Type compliance	3
1.5	Anti-collision	3
2	**Features and benefits**	**4**
2.1	EEPROM	4
3	**Applications**	**5**
4	**Quick reference data**	**6**
5	**Ordering information**	**7**
6	**Block diagram**	**8**
7	**Pinning information**	**9**
7.1	Pinning	9
8	**Functional description**	**10**
8.1	Block description	10
8.2	RF interface	10
8.3	Data integrity	10
8.4	Communication principle	11
8.4.1	IDLE state	12
8.4.2	READY1 state	12
8.4.3	READY2 state	12
8.4.4	ACTIVE state	12
8.4.5	AUTHENTICATED state	13
8.4.6	HALT state	13
8.5	Memory organization	13
8.5.1	UID/serial number	14
8.5.2	Static lock bytes	15
8.5.3	Dynamic Lock Bytes	15
8.5.4	Capability Container (CC bytes)	16
8.5.5	Data pages	17
8.5.6	Memory content at delivery	17
8.5.7	Configuration pages	17
8.6	NFC counter function	20
8.7	ASCII mirror function	21
8.7.1	UID ASCII mirror function	21
8.7.2	NFC counter mirror function	21
8.7.3	SUNCMAC mirror function	22
8.8	SUNCMAC	22
8.8.1	SUNCMAC calculation	22
8.8.2	Programming of the SUNCMAC key	23
8.9	Password verification protection	23
8.9.1	Programming of PWD and PACK	24
8.9.2	Limiting failed authentication attempts	24
8.9.3	Protection of configuration pages	24
8.10	Originality signature	24
8.10.1	Originality Signature at delivery	25
9	**Command overview**	**26**
9.1	NTAG 223 DNA command overview	26
9.2	Timings	26
9.3	NTAG ACK and NAK	27
9.4	ATQA and SAK responses	27
10	**NTAG commands**	**29**
10.1	GET_VERSION	29
10.2	READ	30
10.3	FAST_READ	31
10.4	WRITE	33
10.5	READ_CNT	34
10.6	PWD_AUTH	35
10.7	READ_SIG	36
10.8	WRITE_SIG	37
10.9	LOCK_SIG	38
11	**Limiting values**	**40**
12	**Characteristics**	**41**
13	**Wafer specification**	**42**
13.1	Fail die identification	43
14	**Delivery**	**44**
14.1	Delivery as a wafer	44
14.2	Delivery Method One: The customer collects the product themselves	44
14.3	Delivery Method Two: The Product is sent by NXP and protected by special measures	44
15	**Bare die outline**	**46**
16	**Abbreviations**	**47**
17	**References**	**48**
18	**Revision history**	**49**
19	**Legal information**	**50**

Date of release: 5 April 2023
Document identifier: NT2H2331G0